INTERNATIONAL MARITIME ORGANIZATION

IMO

E

SUB-COMMITTEE ON
RADIOCOMMUNICATIONS AND
SEARCH AND RESCUE
10th session
Agenda item 10

COMSAR 10/10
2 December 2005
Original: ENGLISH

# MEASURES TO ENCHANCE MARITIME SECURITY

## Report of the Correspondence Group on Long-Range Identification and Tracking of Ships

**Submitted by the Co-ordinator of the Correspondence Group**


| SUMMARY | |
|---|---|
| ***Executive summary:*** | This document contains the report of the Correspondence Group on Long-Range Identification and Tracking of Ships |
| ***Action to be taken:*** | Paragraph 4 |
| ***Related documents:*** | COMSAR 9/19, paragraphs 12.50.9 and 12.50.10 and annex 16, COMSAR 9/WP.5/Rev.1, MSC 80/WP.6/Add.3 and MSC 80/24, section 5 |


### Introduction

1 This document contains the annexed report of the Correspondence Group on Long-Range Identification and Tracking (LRIT) of Ships.

### Background

2 COMSAR 9 established the Correspondence Group to address a series of nine questions related to LRIT. At MSC 80, the Committee made some decisions related to LRIT and directed the Correspondence Group to address an additional five questions.

### Discussion

3 The Correspondence Group had volunteers propose draft solutions to each of these 14 questions. Drafts were posted to an e-mail reflector and consensus on each "Task" was reached through e-mail discussions.

### Action requested of the Sub-Committee

4 The Sub-Committee is requested to consider the annexed report of the Correspondence Group and decide as appropriate.

***

# ANNEX

# REPORT OF THE CORRSPONDENCE GROUP ON LONG-RANGE IDENTIFICATION AND TRACKING OF SHIPS

## TASK 1: LRIT INTERNATIONAL DATABASE

### 1 Summary of COMSAR 9's conclusions and guidance to the Correspondence Group

Determine the need for multiple copies of the LRIT international database, widely distributed around the world in order to ensure that the database is robust and able to withstand equipment failure.

### 2 Background material

a. IMSO MSC 80/5/5
b. Marshall Islands MSC 80/5/9
c. European Commission MSC 80/INF.2
d. United States MSC 80/J/19
e. Marshall Islands MSC 80/J/20
f. IMSO MSC 80/J/21
g. MSC 80/WP.6
h. MSC 80/WP.7/Add.1

### 3 Correspondence Group's recommendation

*Background*

Documents MSC 80/5/5 and MSC 80/J/21 present a scenario in which the LRIT international database is *distributed* across three locations world-wide; initially envisioned to be in Australasia, Europe and the Americas. It is argued that this arrangement be adopted to ensure that the database is robust and able to withstand equipment failure, natural disaster or terrorist attack. Data would be fully synchronized across each of the three locations to allow immediate hot-switching in the event of failure of any single or pair of servers. No further detail relating to the proposed architecture was provided.

Documents MSC 80/5/9 and MSC 80/INF.2 (supplemented by MSC 80/J/20) present an alternative scenario in which the LRIT international database is *centralized*; with robustness/reliability achieved through the implementation of a dynamic back-up facility as per standard commercial practice applied across many data critical applications. It suggests that further redundancy could be achieved through the provision of local backup procedures at each Flag State national facility (a simple, small, flat-file database). If required, to counter catastrophic failure in the unlikely event of a natural disaster or malicious destruction, an off-line backup facility could be integrated from a secure specialist server hosting facility (geographically separated from the main database).

*Discussion*

The LRIT international database can be designed to be as simple or as complex as we want it to be. With a centralized architecture, the back-up database should have a separate set of operators trained to handle all daily and regular tasks including maintenance, but they should not be

involved in those activities for other purposes than training, unless an emergency occurs. The operators at the main location should have the facilities for remote operation of the back-up system, and could also be moved to the back-up site if and when required. Both databases should have identical hardware and software, use leased lines for replication and remote control and have individual access points to internet for external access. With a distributed architecture, there is no international database. Each LRIT Data Centre (National, Regional, etc.) will have only the LRIT information it must have: all flag vessels and vessels of other Contracting Governments currently transiting defined areas.

*Summary*

In the absence of any consultative study which determines the cost/benefit of a distributed versus centralized LRIT international database, a pragmatic approach should be taken to achieve an operative LRIT system recognizing the schedule and cost constraints that will inevitably be placed upon the LRIT oversight and operations.

The alternative is to take a complex technical line that however attractive in terms of data security, robustness, reliability, and redundancy, may be problematic due to the cost of design, implementation, operation, and oversight.

The Group recommends that multiple copies of the LRIT international database, widely distributed around the world are not required. To counter catastrophic failure in the unlikely event of a natural disaster or malicious destruction, an off-line backup facility could be integrated from a secure specialist server hosting facility. This facility could be geographically separated from the main LRIT data centre. Local backup procedures at each Flag State national facility will also support disaster recovery.

**TASK 2: DATA SECURITY**

## 1 Summary of COMSAR 9's conclusions and guidance to the Correspondence Group

Determine the requirements for the provision of data security including data encryption, authentication and physical security.

## 2 Background material

COMSAR 8/WP.5 Security aspects
COMSAR 9/19, annex 14 sections 3.6 and 6

## 3 Correspondence Group's response

*Background*

LRIT data security aspects were raised during COMSAR 8. The discussion pointed out that different security requirements need to be applied to the entire LRIT system because the communication interfaces that compose the LRIT system are different. At COMSAR 9 the proposed draft amendment to SOLAS XI-2 included provisional requirement for security data; – in regulation 3.6 "*the means of transmitting information to enable the identification and tracking of a ship shall ensure that the information transmitted by the ship is protected, during transmission from the ship, from unauthorized access or disclosure*;"

and in regulation 6 "*the Contracting Government shall, at all times:*

*.1 recognize and respect the commercial confidentiality and sensitivity of any information they may receive;*

*.2 protect the LRIT information they may receive from unauthorized access or disclosure;*".

The "means of transmitting information" is composed of several segments:

- Ship to Shore: From the ship to the LRIT Service including the communication through a Satellite Service Provider (SSP) and the transfer of the data from the SSP ground based centre to the LRIT Data Centre.

- LRIT Data Centre to the Contracting Government point of Contact.

- Contracting Government interface in charge of routing the data from its National Vessel Monitoring System (NVMS) (in case only one point of contact is linked to the LRIT DC) to the end user (LRIT National Control Centre e.g. MRCC, VTS, MCC, etc.).

- The LRIT DC will also need to interconnect with its backup or disaster recovery site.

*Discussion*

The communication interfaces used for the exchange of LRIT data must be identified for every node in the communication links:

- Ship to shore;
- SSP to LRIT Data Centre (LDC)
- LDC to NVMSs
- LDC to LDC backup.

The ship to shore interface will be supported by the satellite or other viable future communication technology. Due to the technique in use in the space domain, it is not reasonable to envisage imposing any additional requirement regarding the protection of data supported by such system. The satellite provider will have to comply with the basic user requirements regarding the protection of data from unauthorized access or disclosure. The liability implications codified in existing contracts with shipowners and a competitive marketplace ensure satellite providers will continue to make use of the most effective technology to secure data on this portion of the link.

SSP to LDC (and between the LDC and backup site). It is conceivable that the ground communication exchange of LRIT data will be via the Internet. Based on existing communication architecture in use in other maritime applications, Virtual Private Networks (VPN) enable the building of secure private communication networks over a public network infrastructure. The main reasons and motivations are:

- VPN over Internet is a universal and cost effective solution; each LRIT user can choose its own Internet service provider;

- Information must be delivered confidentially with a high level of integrity.

There are many different VPN technologies to choose from. Before adopting a solution, LRIT users have to define their requirements. For a VPN user, such a list will typically include the following criteria:

- VPN service: the VPN service must match the type of service required by the LRIT user.

- Quality of service (QoS): If quality of service for connections between LRIT DCs and LRIT users is required, the service provider backbone must support the provisioning of QoS constrains in term of delay and guarantee of delivery.

- Security: The solution should support encryption, authentication and integrity checking of data in the VPN tunnel or connection for ensuring the end to end integrity and confidentiality. To preclude the downloading of improper or malicious software, only the official web site of the software should be used in conjunction with systems for checking the integrity of the software packages (e.g., MD5).

- Cost: the VPN user may require a solution that does not involve a costly investment. It is open source and may also have the added benefit of not being subject to the export/import regulations of our various countries.

- Manageability: the LRIT user will want an easy to manage solution. The day to day management should not be too onerous. A well designed PKI may address this.

- Scalability/performance: the solution must scale well.

However, the Internet need not be the only method used for ground communication exchange. Alternative interfaces may also be considered to accommodate for national preferences and various infrastructures of each end user and also the options available to the SSP. For example, leased lines, PSTN, various satellite connections, etc. may be available as possible options.

LDC or NVMSs to LRIT end users. The security strategy is directly dependent on the network implemented for the distribution of LRIT data. Due to the nature of the LRIT data, one solution could be the use of the IPsec VPN in tunnelling mode across Internet. This network would support a Public Key Infrastructure (PKI) - a combination of authentication, encryption, and management technologies used to protect the security of communications and transactions on Internet.

*LRIT recommended security measures.* The solutions to secure the traffic flow of the LRIT system should rely on the following security services:

Authorization: Not all data can be made available to every one in the system. The authorization security service ensures the data access is granted only to those who are authorized to see the data. Centralized control of authorization data (e.g., digital certificates, revocation lists) is an effective approach to managing access to the LRIT system. An LRIT user could be identified based on a UserId and a Password or, for greater security, using any one of a number of off-the-shelf 2-factor electronic token systems.

Authentication: An LRIT user application running an application server will exchange messages with the LRIT DC. Using the SSL (Secure Socket layer) protocol can secure the most common application (e.g. Https). It provides data encryption, server authentication, message integrity and optional client authentication as well. A complete PKI with IMO as the Certification Authority can be easily created using off the shelf software to provide automated authentication, encryption, and oversight control through Certificate Revocation Lists and Online Certificate Status Protocol.

Confidentiality: Confidentiality ensures that information is not disclosed to unauthorized people when it travels across the system. The 2 way SSL (such as Transport Layer Security (TLS) [RFC2246]) can be used with PKI for encrypting the traffic between the LRIT DC and the end user.

Integrity: Integrity guarantees that no data has been altered (using HTTPS, SSL, TLS, IPSEC, etc).

## TASK 3: REQUESTING LRIT INFORMATION DIRECTLY FROM AN LRIT TRACKING SERVICE

### 1 Summary of COMSAR 9's conclusions and guidance to the Correspondence Group

Determine whether a Contracting Government should be permitted to request LRIT information directly from an LRIT Tracking Service on any ship for which they are entitled to obtain LRIT information, or whether requests for information directly from LRIT Tracking Services should be limited to Administrations seeking information on ships flying their flag.

### 2 Background material

Documents MSC 80/24 Final Report (paragraphs 5.67, 5.94 to 5.97 and 5.104)

### 3 Correspondence Group's response

a. Each Administration should be able to receive all LRIT data for all the ships entitled to fly its flag irrespective of where such ships may be.

b. In accordance with document MSC 80/24, paragraph 5.94, the LRIT architecture should not allow a ship to transmit LRIT information directly to a port or a coastal State.

c. Governments should have enough flexibility while meeting IMO LRIT requirements to implement a structure which is acceptable for national regulations. To that end, the LRIT architecture should allow for interfacing with national vessel monitoring systems and not prevent the Administration from obtaining LRIT information from the national vessel monitoring system.

**TASK 4: ARCHIVING LRIT INFORMATION**

## 1 Summary of COMSAR 9's conclusions and guidance to the Correspondence Group

Determine whether the LRIT Data Centre or LRIT Tracking Services should have the capability to archive LRIT information, and if so, for how long.

## 2 Background material

Input from various Vessel Traffic Services, Maritime Domain Awareness, and Search and Rescue programs

## 3 Correspondence Group's response

The LRIT system should have the ability to archive and retrieve archived/recorded information, whether for immediate playback or for post-event retrieval. Archival of LRIT information may be accomplished at several nodes within an LRIT system. These nodes include: 1) the shipboard terminal; 2) the downlink site of the communications service provider (i.e., land earth station); 3) LRIT Data Centre; and/or 4) Contracting Governments.

Shipboard Terminal: Although the LRIT shipboard terminal could have the ability to archive data, many ships already have the capability to receive, record, and archive this type of information for use at a later time. For example, Electronic Chart Display and Information Systems (ECDIS) may have this capability and therefore, it is likely not required for the LRIT shipboard terminal.

Communications Service Provider: Archiving requirements will be determined by the commercial entity operating the communications link. This could also be a market-driven requirement, i.e., if the LRIT Data Centre or LRIT Service requires the communications service provider to archive data, the communications service provider, if capable, may elect to provide additional archiving capability to the LRIT system at an additional cost for this service. Due to the transient nature of the data at the communications service provider, the retention of this data should not be required to be archived longer than [4] days.

LRIT Service Provider: The LRIT Service Provider provides the link between the communications service provider and the LRIT Data Centre. In this role, and absent an archiving capability provided by the communications service provider, the LRIT Service provider must have an archiving capability for LRIT information up to [45] days. However, there may be national requirements placed on LRIT Service Providers that are more stringent than LRIT requirements. For example, under the UK National Data Protection Act 1998, personal data (such as the Company Security Officer name/contact details, and Account names/contact details) must be retained for a period of 7 years. National obligations may vary, specifically the distinction between personal and non-personal data (e.g., ship position information), and the period of retention. Furthermore there may be waiver conditions applied to organizations (e.g., IMO).

LRIT Data Centre: The LRIT Data Centre is the heart of the LRIT system and will likely need archiving capability. The frequency of archived reports and the length of time these reports are retained should depend on the function. In order to carry out its oversight role, the LRIT Oversight Organization must have access to archived information to determine if the LRIT Data Centre has provided access to LRIT information to appropriately validated Contracting Governments (Flag, Port, Coastal States) and these entities have been billed accordingly.

Therefore, LRIT Service Providers should archive LRIT information for [365] days. Additionally, the LRIT Data Centre should archive track data for the previous [10] [voyages] [transits] of each ship. Furthermore, Contracting Governments may wish to specify the period of time in which the archived LRIT data should be available to them upon request to the LRIT Data Centre, for example:

- For LRIT information within the last [4days], the LRIT DC should resend LRIT data within [30 min];

- In the last [30] days, the LRIT DC should resend a LRIT data within [1hour]; and

- After [30days], the LRIT DC should resend the LRIT data within [5days].

For Flag States that prefer to go directly to the service provider (in the case of a national vessel monitoring system), the archiving arrangement is at the agreement of the Administration and the service provider, but is outside the scope of the overall LRIT system.

Contracting Governments: Whether Flag, Port, or Coastal State, a Contracting Government may elect to archive LRIT information as it sees fit.

## TASK 5: DESTRUCTION OF ARCHIVED LRIT MATERIAL

### 1 Summary of COMSAR 9's conclusions and guidance to the Correspondence Group

Develop protocols for the destruction of archived LRIT material after a time period to be determined.

### 2 Background material

See Task 4.

### 3 Correspondence Group's response

Archived LRIT data may be purged from the archive, following appropriate procedures. Archival and destruction of LRIT information may be accomplished at several nodes within the LRIT system. The LRIT system nodes include: 1) the shipboard terminal; 2) the downlink site of the communications service provider (e.g., land earth station); 3) LRIT Data Centre; and/or 4) Contracting Governments.

Shipboard Terminal: Although the LRIT shipboard terminal could have the ability to archive data, many ships already have the capability to receive, record, and archive this type of information for use at a later time. If this data is archived at the LRIT shipboard terminal, it may be purged according to the operating requirements of the ship master or shipowner.

Communications Service Provider: Archiving requirements will be determined by the commercial entity operating the communications link. Due to the transient nature of the data at the communications service provider, the retention of this data should not be required to be archived longer than [4] days. Destruction of this data will be determined by the individual communications service providers.

LRIT Service Provider: The LRIT Service Provider provides the link between the communications service provider and the LRIT Data Centre. Absent an archiving capability provided by the communications service provider, the LRIT Service provider must have an archiving capability for LRIT information up to [45] days. Destruction of data held by the LRIT Service Provider should be performed in concert with the LRIT Data Centre to ensure that the Centre has archived this data. However, there may be national requirements placed on LRIT Service Providers that are more stringent than LRIT requirements. For example, under the UK National Data Protection Act 1998, personal data (such as the Company Security Officer name/contact details, and Account names/contact details) must be retained for a period of 7 years. National obligations may vary, specifically the distinction between personal and non-personal data (e.g., ship position information), and the period of retention. Furthermore there may be waiver conditions applied to organizations (e.g., IMO).

LRIT Data Centre: The LRIT Data Centre is the heart of the LRIT system and will need archiving capability. In order to carry out its oversight role, the LRIT Oversight Organization should have access to LRIT Data Centre's archived information to determine if the LRIT Data Centre has provided access to LRIT information to appropriately validated Contracting Governments (Flag, Port, Coastal States) and these entities have been billed accordingly. Therefore, LRIT Service Providers should archive LRIT information for [365] days. Additionally, the LRIT Data Centre should archive track data for the previous [10] [voyages] [transits] of each ship. The LRIT Data Centre may destroy data that is older than [365] days.

[Transits] [voyages] older than [365] days that are not in the latest 10 [transits] [voyages] may be purged.

For Flag States that prefer to go directly to the service provider (in the case of a national vessel monitoring system), the archiving and destruction arrangement is at the agreement of the Administration and the service provider, but is outside the scope of the overall LRIT system.

Contracting Governments: Whether Flag, Port, or Coastal State, a Contracting Government may elect to destroy LRIT information it holds as it sees fit.

## TASK 6: LRIT INFORMATION LATENCY

### 1 Summary of COMSAR 9's conclusions and guidance to the Correspondence Group

Determine whether or not there should be a limitation for LRIT information latency, and if there should be, what that limitation should be (Five minutes? One hour? Near real time?).

### 2 Background material

First, LRIT information latency should be defined. There are essentially 2 parts to latency:

- The time taken for the information to travel from the vessel, over the satellite, through the land earth station to the LRIT provider (Figure 1, Label 1).

- The time taken for the information to travel from the LRIT provider across the distribution network to the LRIT Client (Label 2).

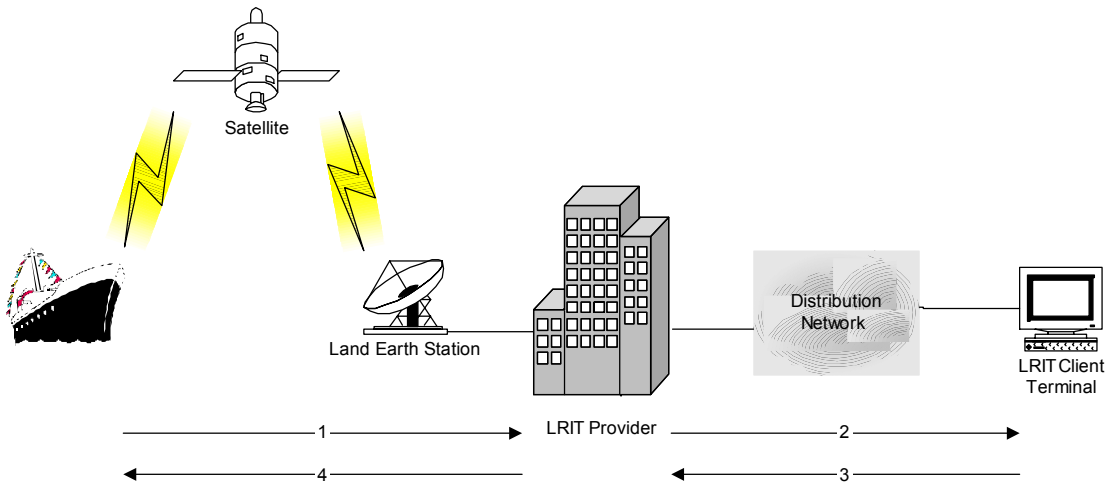


**Figure 1. Basic LRIT System Schematic**

There are essentially 3 types of LRIT messages and each should have different latency requirements:

- Pre-scheduled position report
- On-demand (polled)
- Event message

For a pre-scheduled position reports, latency should be regarded as Label 1 in Figure 1. For an event message, Labels 1 and 2 are applicable. For an on-demand position report (polled message and reply), Labels 3 and 4 are for the poll, plus the response time at the vessel, and labels 1 and 2 for the reply.

***Implications of Latency***

Table 1 shows the implied error in position that has to be tolerated for a vessel moving at a certain speed with the amount of latency for pre-scheduled reports. It should be noted that these latency performances could be achieved with current technology.

| Vessel Speed (knots) | Latency | | | | | |
|---|---|---|---|---|---|---|
| | NRT(30sec) | 5 min | 15 min | 30 min | 1 hr | 4 hr |
| 12 | 0.09 nm | 0.99 nm | 3.00 nm | 5.99 nm | 11.9 nm | 48.0 nm |
| 15 | 0.12 nm | 1.24 nm | 3.74 nm | 7.50 nm | 15.0 nm | 59.9 nm |
| 24 | 0.19 nm | 1.99 nm | 5.99 nm | 11.9 nm | 24.0 nm | 96.1 nm |
| 32 | 0.26 nm | 2.64 nm | 7.99 nm | 15.9 nm | 32.0 nm | 128 nm |

**Table 1. Positional Error Possibilities – Latency vs. Speed (NRT – Near Real Time, which can be up to 30 seconds latency)**

As with all wireless systems, there is a possibility that a pre-scheduled position report may be lost and thus these errors would be doubled. In addition, for on-demand position reports, the position error may be twice the amount. (See Table 2).

| Vessel Speed (knots) | Latency | | | | | |
|---|---|---|---|---|---|---|
| | NRT(30sec) | 5 min | 15 min | 30 min | 1 hr | 4 hr |
| 12 | 0.19 nm | 1.99 nm | 5.99 nm | 11.9 nm | 24.0 nm | 96.1 nm |
| 15 | 0.25 nm | 2.49 nm | 7.50 nm | 15.0 nm | 30.0 nm | 120 nm |
| 24 | 0.39 nm | 3.99 nm | 11.9 nm | 24.0 nm | 48.0 nm | 192 nm |
| 32 | 0.53 nm | 5.29 nm | 15.9 nm | 32.0 nm | 64.2 nm | 256 km |

**Table 2. Positional Error Possibilities – loss of one pre-scheduled position report or for on-demand position report**

Other implications of latency are the ability to manage situations and whether the terminal is used for other purposes. The on-demand report latency directly affects the ability to manage situations, requiring a near-real-time operation. If the terminal is used for other purposes, it may only respond when it completes other transmissions. Furthermore, the latency through a distribution network can be significant, but most of the latency will be between the vessel and the LRIT service provider. In order to minimize the latency through the distribution network, high bandwidth, high availability links should be maintained, with fast encryption services.

## 3 Correspondence Group's response

*Recommendations*

Operational requirements and situation management require a limitation on maximum latency for LRIT information. For pre-scheduled message and position reports as well as event messages, the maximum latency should be [5] minutes [95%] of the time per 24 hour period and [99%] over a month period. However, for the other messages such as on-demand, latency will double due to the fact that the message will take [5] minutes to get there and at least [5] minutes for a reply, giving a [10] minute maximum latency before a reaction can be executed. A dedicated terminal should be required for LRIT. If the terminal is performing any other function, latency can increase.

*Summary*

The acceptable latency based on operational requirements, and as technology is able to provide, is [5] minutes for pre-scheduled and event messages. For poll and reply messages, the latency will double to [10] minutes. The quality of service should be [95%] of the time over a 24-hour period and [99%] over 1-month.

## TASK 7: LRIT REQUIREMENTS IN SOLAS OR PERFORMANCE STANDARDS

### 1 Summary of COMSAR 9's conclusions and guidance to the Correspondence Group

Determine which requirements related to LRIT should be included in the SOLAS provisions and which should be included in the performance standards for LRIT, so as to avoid conflicting or overlapping requirements.

### 2 Background material

MSC 80 established an intersessional working group to prepare draft SOLAS amendment for LRIT. Accordingly, the Group did not address SOLAS text but concentrated on LRIT functional requirements and performance standards in this Task.

### 3 Correspondence Group's response

#### 1 *Scope*

The purpose of this document is to describe the functional requirements for the delivery of Long Range Identification and Tracking (LRIT) data to Contracting Governments.

#### 2 *Roles and Responsibilities*

In defining the requirements from the perspective of "End User" it is important to recognize the roles and responsibilities of the key "players" proposed for the delivery of LRIT services. A brief summary is provided below.

| | |
|---|---|
| **LRIT Co-ordinator** | • Oversees LRIT Data Centre(s) which enables Contracting Governments to obtain LRIT information they are entitled to receive.<br>• Ensures that Contracting Governments receive only the LRIT information that they are entitled to receive.<br>• Ensures that Contracting Governments only pay for the LRIT information that they have requested and received.<br>• Identifies the format and manner in which LRIT information is provided to Contracting Governments. |
| **LRIT Application Service Provider (ASP)** | • LRIT ASPs are IMO approved services for the delivery of tracking data to Contracting Governments. A vessel may use any recognized LRIT ASP acceptable to the Administration |
| **LRIT Data Centre(s)**<br><br>**(National or International)** | • Collects LRIT information continuously from all vessels, via the LRIT ASPs.<br>• Offers to contract with all Contracting Governments to provide access to LRIT information.<br>• Maintains data connections with other LRIT Data Centre(s).<br>• Prescribes the manner in which Contracting Governments pay for LRIT information.<br>• Provides LRIT Data to each Contracting Government upon demand and when entitled to the information. |
| **International LRIT Data Network** | • Network supporting data interchange between National LRIT Data Centres |

| | |
|---|---|
| **Contracting Governments (Administrations)** | • LRIT information is supplied to Contracting Governments entitled to receive the information through the LRIT Data Centre. Contracting Governments may also obtain information on vessels flying their flag directly from LRIT ASPs or a national vessel monitoring system. |
| **Vessel** | • Vessels are responsible for the installation of the prescribed equipment. |
| **Prescribed Equipment** | • Prescribed LRIT equipment onboard vessels as determined by SOLAS Amendment and Performance Standards. |

## 3 *Introduction*

All ships (*subject to the SOLAS regulation*) must be capable of transmitting an LRIT report to an LRIT Tracking Service.

There is a diversity of existing equipment onboard vessels that offer long-range communication and reporting capabilities and it is recognized that all existing equipment may not meet adequate functionality or levels of data integrity for position reporting within a security environment.

To facilitate the scheduled introduction of LRIT and ensure all ships (*subject to the SOLAS regulati*on) have equipment that can deliver the essential requirements necessary to ensure the robust and accurate delivery of LRIT reports within a security environment it is recommended that a grandfather clause be included in the Functional Requirements to allow for a phased in approach over a [1 – 2] year time scale.

Subsequently, throughout this document two levels of functional requirements are described. That is:

**Level 1 Functionality -** defines a level of LRIT capability that provides a basic level of functionality, data quality and integrity as prescribed in Section 4. With the introduction of LRIT all ships (*subject to the SOLAS regulation*) must have operational equipment onboard that meets Level 1 Functionality.

**Level 2 Functionality -** defines a level of LRIT capability that provides an acceptable level of functionality, data quality and integrity as prescribed in Section 4. With the introduction of LRIT it is recommended that all ships (*subject to the SOLAS regulation*) have operational equipment onboard that meets Level 2 Functionality within a defined time schedule [1 – 2 year time scale]. A summary of the Level 1 and Level 2 functional requirement is provided in annex 1.

## 4 *Key Requirements*

The following items should be included in defining LRIT Requirements.

- Data Items
- Prescribed Equipment
- System Integrity
- Functional Requirements for LRIT ASPs

4.1 *Data Items to be provided to contracting governments*

4.1.1 Key Data Items required

***Level 1 Functionality***

The data items to be provided to Contracting Governments by LRIT Data Centres for Level 1 Functionality includes:

| Data Source | Parameter | Comments |
|---|---|---|
| **Data to be transmitted from the onboard equipment** | Unique equipment Identifier | The Identifier used by the onboard transmitting equipment. |
| | Position | The GNSS position (latitude and longitude) of the vessel (WGS84). |
| | Time Stamp 1 | The time (UTC) associated with the GNSS position. |
| **Data to be added by the LRIT ASP** | LRIT ASP Identifier | The identity of the LRIT ASP to be clearly identified by an approved Unique Identifier |
| | Vessel Identity[1] | The IMO number and MMSI number for the vessel. |
| | Time Stamp 2 | The time the position report is received by the LRIT ASP. |
| | Time Stamp 3 | The time the position report is forwarded from the LRIT ASP to an LRIT Data Centre. |
| **Data to be added by the LRIT Data Centre** | LRIT Data Centre Identifier | The identity of the vessel to be clearly identified by an approved Unique Identifier. |
| | Vessel Identify[1] | The data forwarded from the LRIT Data Centre to Contracting Governments is to include the IMO number and MMSI number for the vessel. |
| | Time Stamp 4 | The time the position report is received by the LRIT Data Centre. |
| | Time Stamp 5 | The time the position report is forwarded from the LRIT Data Centre to a contracting government. |

[1] **Note**: Either the LRIT ASP or the LRIT Data Centre may add the vessel identity but the responsibility to ensure the data item is added rests with the LRIT Data Centre.

These data items are henceforth referred to as "LRIT data".

Where LRIT equipment meets Level 1 Functionality and also provides additional information such as described in Level 2 Functionality the provision of these items may be negotiated between the LRIT Data Centre and Contracting Governments if the LRIT equipment provides them.

***Level 2 Functionality***

Many potential users of LRIT data have requested additional data items to be included with the LRIT data provided to Contracting Governments by LRIT Data Centres. Recognizing this and the need to minimize the requirement for vessels to be fitted with additional or new equipment or to install new or to modify or upgrade existing software already installed onboard it is recommended that consideration be given to including additional items for Level 2 Functionality.

These items may not necessarily be mandatory LRIT data under Level 2 requirements.

The items to be considered for Level 2 Functionality include:

| Parameter | Comments |
|---|---|
| Status Code | Status Code to reflect the status of the data report (i.e. whether it is a normal position report or a system integrity check has been activated (see section 4.2.8) |
| Speed | Instantaneous GNSS speed from the GNSS Unit onboard the LRIT equipment |
| Course | Instantaneous GNSS heading from the GNSS Unit onboard the LRIT equipment |
| Other? | For example, destination. |

In the interim it is recommended that provision of these items may be negotiated between the LRIT Data Centre and Contracting Governments if the LRIT equipment provides them.

4.1.2 Data Format

This requirement recognizes that the format/s used by existing and emerging equipment suppliers and LRIT providers may differ but ensures that LRIT data is delivered to contracting governments in a single fixed format data structure.

| Data Source | Parameter | Format |
|---|---|---|
| **Data to be transmitted from the onboard equipment** | Unique equipment Identifier | <To be defined> |
| | Position | <To be defined> |
| | Time Stamp 1 | <To be defined> |
| **Data to be added by the LRIT ASP** | LRIT ASP Identifier | <To be defined> |
| | Vessel Identity[1] | <To be defined> |
| | Time Stamp 2 | <To be defined> |
| | Time Stamp 3 | <To be defined> |
| **Data to be added by the LRIT Data Centre** | LRIT Data Centre Identity | <To be defined> |
| | Vessel Identity[1] | <To be defined> |
| | Time Stamp 4 | <To be defined> |
| | Time Stamp 5 | <To be defined> |

[1] **Note**: Either the LRIT ASP or the LRIT Data Centre may add the vessel identity but the responsibility to ensure the data item is added rests with the LRIT Data Centre.

***Additional Data Items***

Where a contracting government seeks additional items from LRIT equipment with such capabilities the data format is to be negotiated between the Contracting Government and the LRIT Data Centre.

4.2 *Prescribed LRIT Equipment*

The requirements for prescribed equipment onboard vessels, as determined by SOLAS Amendment and Performance Standards, are provided below.

4.2.1 Data Elements

LRIT equipment must be capable of providing the following mandatory data elements to LRIT ASPs for both Level 1 and Level 2 Functionality:

| Parameter | Comments |
|---|---|
| Unique equipment Identifier | The Identifier used by the onboard transmitting equipment. |
| Position | The GNSS position (latitude and longitude) of the vessel (WGS84) |
| Time Stamp 1 | The time (UTC) associated with the GNSS position |

4.2.2 Equipment Identifier

The prescribed equipment must be capable of transmitting the identifier used by the onboard transmitting equipment to an LRIT ASP, irrespective of where the vessel is located.

4.2.3 Positional Data

The equipment must be capable of transmitting the position of the vessel to an LRIT ASP, irrespective of where the vessel is located under the following guidelines:

| Level of Functionality | Functionality Required |
|---|---|
| Level 1 Functionality | **1. Position Data**<br>The equipment must be capable of transmitting the GNSS position (latitude and longitude) of the vessel (WGS84) as prescribed by the *SOLAS regulation*, without human interaction on board the vessel. |
| | **2. On-Demand Position Reports**<br>The equipment must be capable of responding to a request to forward position data on demand without human interaction onboard the vessel, irrespective of where the vessel is located. |
| | **3. Pre-scheduled Position Reports**<br>The equipment must be capable of being remotely configured to forward position reports at intervals ranging from a minimum of [15] minutes to periods of 24 hours and greater to LRIT ASPs, irrespective of where the vessel is located and without human interaction on board the vessel. |
| Level 2 Functionality | **1. Position Data**<br>The equipment must be capable of transmitting the GNSS position (latitude and longitude) of the vessel (WGS84) as prescribed by the *SOLAS regulation*, without human interaction on board the vessel. |
| | **2. On-Demand Position Reports**<br>The equipment must be capable of responding to a request to forward position data on demand without human interaction onboard the vessel, irrespective of where the vessel is located and without human interaction on board the vessel. |
| | **3. Pre-scheduled Position Reports**<br>The equipment must be capable of being remotely configured to forward position reports at intervals ranging from a minimum of [15] minutes to periods of 24 hours and greater to LRIT ASPs, irrespective of where the vessel is located and without human interaction on board the vessel. |
| | **4. Stop Reporting**<br>The equipment must be capable of responding to a request to cease forwarding Pre-scheduled Position Reports without human interaction onboard the vessel, irrespective of where the vessel is located. |

4.2.4 Time Stamp

The prescribed equipment must be capable of forwarding the time (UTC) associated with the GNSS position with each LRIT data report forwarded to the LRIT ASP.

4.2.5 Coverage

The prescribed equipment must be capable of delivering LRIT functionality for those Sea Areas in which the ship is certified to operate in accordance with SOLAS Chapter IV. These include Sea Areas A1, A2, A3 and A4 as defined in regulations IV/2.1.12, IV/2.1.13, IV/2.1.14, and IV/2.1.15).

4.2.6 Latency

Operational requirements and situation management require a limitation on maximum latency for LRIT information. Within the reporting requirements prescribed by the SOLAS amendment LRIT Equipment must be capable of delivering LRIT data to LRIT ASPs in near real time irrespective of where the vessel is located. In particular, this includes:

1. For pre-scheduled position reports the latency for forwarding LRIT data to LRIT ASP must be [5] minutes or less.

2. For "On demand" position reports and messaging the latency for forwarding LRIT data to LRIT ASP must be [10] minutes or less.

3. The availability of service should be [95%] of the time over a 24-hour period and [99%] over 1-month.

4.2.7 Physical Security of Prescribed Equipment

LRIT equipment must be capable of meeting the following physical security capabilities for Level 1 and Level 2 Functionality.

| **Level of Functionality** | **Functionality Required** |
|---|---|
| Level 1 Functionality | 1. The equipment must be capable of transmitting the GNSS position (latitude and longitude) of the vessel (WGS84) as prescribed by the *SOLAS regulation*, without human interaction on board the vessel. |
| Level 2 Functionality | 1. The equipment must be capable of transmitting the GNSS position (latitude and longitude) of the vessel (WGS84) as prescribed by the *SOLAS regulation*, without human interaction on board the vessel.<br><br>2. Prescribed LRIT equipment must include the capability to provide robust protection against wilful attempts to compromise the physical security of the equipment or readily allow the equipment to be modified in a manner that would enable false data to be transmitted, such as the vessel appears to be in a different location. |

| Level of Functionality | Functionality Required |
|---|---|
| | Key elements required of the equipment to minimize such events include:<br><br>i. The equipment must have an internal GNSS<br>ii. The internal GNSS to be configured for WGS84<br>iii. The internal GNSS must override any external position source or provision to enter manual position reports<br>iv. The GNSS and data communications applications of equipment should be highly integrated so that the link between them may not be readily accessed in manner that may compromise the integrity of the data to be transmitted from the LRIT equipment |

4.2.8 Concurrent Users

***Level 1 Functionality***

There are no requirements for LRIT equipment to have a capability to provide a multi-tasking environment that is capable of supporting the needs of multiple, independent and concurrent users providing the equipments meets Level 1 Functionality as defined in Section 4.1.

***Level 2 Functionality***

The equipment must provide a multi-tasking environment that is capable of supporting the needs of multiple, independent and concurrent users. That is, equipment must be capable of being remotely and independently configured by more than one authorized body to forward data. For example the vessel's owner and a port authority may simultaneously use the equipment for position reporting at different intervals concurrently with the LRIT Data Centre(s) on behalf of a Contracting Government for LRIT purposes.

A minimum number of concurrent independent users the equipment should be capable of supporting is included in the performance standards for prescribed equipment.

The number of concurrent users allowed should also be configurable on the equipment. For example the equipment may be capable of many concurrent users but the master may wish to restrict the availability of the equipment to certain users only.

4.2.9 Status of Prescribed Equipment

***Level 1 Functionality***
There are no requirements for LRIT equipment to have a capability to provide status messages describing the status of the equipment providing the equipments meets Level Functionality as defined in Section 4.1.

***Level 2 Requirements***

Level 2 Functionality should include the capability for prescribed equipment to automatically provide basic information to the LRIT ASP with regards to the status of the equipment onboard a vessel. Suggest that this includes the status of Power Supply and Antenna Availability.

**Power Supply**

The equipment must be capable of providing a position report and a status message identifying the status of power to the equipment. This is to include:

1. **Power On** – The equipment must be capable of automatically forwarding a 'Power On' message to the LRIT Data Centre when it is turned on after power is restored. This message should also include a position report as outlined in Section 2.1.

2. **Power Off** – The equipment must be capable of forwarding a 'Power Off' message when the equipment has been deliberately shut-down (e.g. via the unit being deliberately powered off using the menu features or power is lost abruptly). This message should also include a position report as outlined in Section 2.1.

   These Status Messages can either be forwarded during a system shutdown or in association with the next Power On message.

**Antenna Availability**

The equipment must be capable of detecting when the antenna is disconnected or otherwise prevented from establishing communications with the LRIT ASP.

1. **Antenna Disconnect** – The equipment must be capable of forwarding an 'Antenna Disconnect' status when an antenna is disconnected. This event must be recognized and forwarded whenever the antenna is reconnected. This message should also include a position report as outlined in Section 2.1.

2. **Antenna blocked –** The equipment must be capable of forwarding an 'Antenna blocked' status when an antenna is blocked and unable to establish communications. This event must be recognized and forwarded whenever the antenna is un-blocked. This message should also include a position report as outlined in Section 2.1.

4.2.10 Future Capabilities

**'Health' Check of Prescribed Equipment**

It is recommended that with the introduction of Level 2 Functionality that it be a requirement for new equipment (new models, etc) to have a capability to provide a status message to the LRIT ASP at regular intervals, or on demand, that indicates the 'health' of the equipment. Similarly, the equipment must have the capability to provide this information onboard the vessel when the equipment fails. It is not clear if this is possible with existing tracking equipment but it should be considered as a future requirement that is phased in. A message providing an indication of the 'health' of the equipment in terms of power supply, clock, GNSS, etc would be an extremely useful diagnosis tool.

4.3 *LRIT Application Service Providers (ASPs)*

Key Functional Requirements for the LRIT ASP include:

4.3.1 Data Elements

LRIT ASPs must be capable of adding the following data elements to the data received from Prescribed LRIT Equipment:

| Parameter | Comments |
|---|---|
| LRIT Tracking Service Identifier | The identity of the LRIT ASP to be clearly identified by an approved Unique Identifier |
| Vessel Identity[1] | The IMO number and MMSI number for the vessel |
| Time Stamp 2 | The time (UTC) the report was received by the LRIT ASP |
| Time Stamp 3 | The time (UTC) the report was forwarded to the LRIT Data Centre. |

[1] **Note**: Either the LRIT ASP or the LRIT Data Centre may add the vessel identity but the responsibility to ensure the data item is added rests with the LRIT Data Centre.

4.3.2 Interface with LRIT Data Centres

LRIT ASP must be capable of processing all prescribed configuration requests for LRIT data from LRIT Data Centres.

4.3.3 Latency

LRIT Data Centres must be capable of:

a) Transmitting LRIT data to LRIT Data Centres in "real time" following the receipt of LRIT Data from individual vessels [less than or equal to 1 minute]; and

b) Responding to requests from LRIT Data Centres for LRIT data from vessels in "real time" [less than or equal to 1 minute].

4.3.4 System Integrity

LRIT ASPs must be capable of monitoring the integrity of LRIT data in terms of accuracy, reliability and latency. While such capability will assist to diagnose wilful attempts to compromise the validity of the data being transmitted it will provide invaluable diagnostic information LRIT ASPs, LRIT Data Centres and contracting governments where there are genuine problems/faults.

4.3.5 Positional Accuracy

The positional data received by the LRIT Tracking Service is to be monitored to detect a faulty GNSS unit on the equipment.

4.3.6 Time Stamp Accuracy

The Time Stamps provided by both the equipment and the LRIT Equipment, LRIT Tracking Service and the LRIT Data Centres must be monitored.

4.3.7 System Availability

<To Follow>

4.4 *LRIT Data Centres*

Key Functional Requirements for the LRIT Data Centres include:

4.4.1 Data Elements

LRIT Data Centres must be capable of adding the following data elements to the data received from LRIT ASPs:

| Parameter | Comments |
|---|---|
| LRIT Data Centre Identifier | The identity of the vessel to be clearly identified by an approved Unique Identifier. |
| Vessel Identify[1] | The data forwarded from the LRIT Data Centre to Contracting Governments is to include the IMO number and MMSI number for the vessel. |
| Time Stamp 4 | The time (UTC) the LRIT report was received by the LRIT Data Centre. |
| Time Stamp 5 | The time (UTC) the data report was forwarded from the LRIT Data Centre to the Contracting Government to each LRIT data report. |

[1] **Note:** Either the LRIT ASP or the LRIT Data Centre may add the vessel identity but the responsibility to ensure the data item is added rests with the LRIT Data Centre.

4.4.2 Configuration Capabilities

LRIT Data Centre(s) must have the capability to request LRIT ASPs to remotely configure prescribed equipment to forward LRIT information as described in Section 4.2.3, irrespective of where a vessel is, and to subsequently receive LRIT information from that vessel irrespective of where it transits.

4.4.3 Interface for Contracting Governments

LRIT Data Centre(s) must be capable of receiving configuration requests for LRIT data from contracting governments in a standard, fixed format.

| Request | Format |
|---|---|
| On Demand Position Reports | <To be defined> |
| Pre-Scheduled Position Reports | <To be defined> |
| Stop Reporting | <To be defined |

4.4.4 Latency

LRIT Data Centres must be capable of:

a) Transmitting LRIT data to contracting governments in “real time” following the receipt of the report from individual vessels [less than or equal to 1 minute]; and

b) Responding to requests from Contracting Governments for LRIT data from LRIT ASPs in “real time” [less than or equal to 1 minute]

4.4.5 System Availability

<To Follow>

Table 1: Summary of the key requirements for Level 1 and Level 2 functionality

| Equipment / Provider | Parameter | | Comments | Functionality | |
|---|---|---|---|---|---|
| | | | | Level 1 | Level 2 |
| **Prescribed LRIT Equipment** | **Data Elements** | **Unique equipment Identifier** | The Identifier used by the onboard transmitting equipment. | **Y** | **Y** |
| | | **Position** | The GNSS position (latitude and longitude) of the vessel (WGS84) | **Y** | **Y** |
| | | **Time Stamp 1** | The time (UTC) associated with the GNSS position | **Y** | **Y** |
| | ***Potential Data elements to be considered (See Section 4.1.1)*** | ***Status Code*** | *Status Code to reflect the status of the data report (i.e. whether it is a normal position report or a system integrity check has been activated (See section 4.2.8)* | | |
| | | ***Speed*** | *Instantaneous GNSS speed from the GNSS Unit onboard the LRIT equipment* | | |
| | | ***Course*** | *Instantaneous GNSS heading from the GNSS Unit onboard the LRIT equipment* | | |
| | | ***Other?*** | *For example, destination.* | | |
| | **Positional Data** | **Position** | The equipment must be capable of transmitting the GNSS position (latitude and longitude) of the vessel (WGS84) as prescribed by the *SOLAS regulation*, without human interaction on board the vessel. | **Y** | **Y** |
| | | **On-Demand Position Reports** | The equipment must be capable of responding to a request to forward position data on demand without human interaction onboard the vessel, irrespective of where the vessel is located. | **Y** | **Y** |
| | | **Pre-scheduled Position Reports** | The equipment must be capable of being remotely configured to forward position reports at intervals ranging from a minimum of [15] minutes to periods of 24 hours and greater to LRIT Tracking Services, irrespective of where the vessel is located and without human interaction on board the vessel | **Y** | **Y** |
| | | **Stop Reporting** | The equipment must be capable of responding to a request to cease forwarding Pre-scheduled Position Reports without human interaction onboard the vessel, irrespective of where the vessel is located | | **Y** |
| | **Time Stamp** | | The prescribed equipment must be capable of forwarding the time (UTC) associated with the GNSS position with each LRIT data report forwarded to the LRIT Tracking Service | **Y** | **Y** |
| | **Coverage** | | The prescribed equipment must be capable of delivering LRIT functionality for those Sea Areas in which the ship is certified to operate in accordance with SOLAS Chapter IV. These include Sea Areas A1, A2, A3 and A4 as defined in regulations IV/2.1.12, IV/2.1.13, IV/2.1.14, IV/2.1.15) | **Y** | **Y** |
| | **Latency** | | Operational requirements and situation management require a limitation on maximum latency for LRIT information.<br>Within the reporting requirements prescribed by the SOLAS amendment LRIT Equipment must be capable of delivering LRIT data to LRIT ASPs in near real time irrespective of where the vessel is located. In particular, this includes:<br>1. For pre-scheduled position reports the latency for forwarding LRIT data to LRIT ASPs must be [5] minutes or less.<br>2. For "On demand" position reports and messaging the latency for forwarding LRIT data to LRIT ASPs must be [10] minutes or less.<br>3. The availability of service should be [95%] of the time over a 24-hour period and [99%] over 1-month | **Y** | **Y** |
| | **Physical Security of Prescribed Equipment** | | The equipment must be capable of transmitting the GNSS position (latitude and longitude) of the vessel (WGS84) as prescribed by the *SOLAS regulation*, without human interaction on board the vessel. | **Y** | **Y** |

| Equipment / Provider | Parameter | Comments | Functionality | |
|---|---|---|---|---|
| | | | Level 1 | Level 2 |
| | | Prescribed LRIT equipment must include the capability to provide robust protection against wilful attempts to compromise the physical security of the equipment or readily allow the equipment to be modified in a manner that would enable false data to be transmitted, such as the vessel appears to be in a different location.<br><br>Key elements required of the equipment to minimize such events include:<br><br>i. The equipment must have an internal GNSS<br><br>ii. The internal GNSS to be configured for WGS84<br><br>iii. The internal GNSS must override any external position source or provision to enter manual position reports<br><br>iv. The GNSS and data communications applications of equipment should be highly integrated so that the link between them may not be readily accessed in manner that may compromise the integrity of the data to be transmitted from the LRIT equipment | | **Y** |
| | **Concurrent Users** | The equipment must provide a multi-tasking environment that is capable of supporting the needs of multiple, independent and concurrent users. That is, equipment must be capable of being remotely and independently configured by more than one authorized body to forward data. For example the vessel's owner and a port authority may simultaneously use the equipment for position reporting at different intervals concurrently with the LRIT Data Centre(s) on behalf of a Contracting Government for LRIT purposes | | **Y** |
| | **Status of Prescribed Equipment** | LRIT Equipment functionality should include the capability for prescribed equipment to automatically provide basic information to the LRIT ASP with regards to the status of the equipment onboard a vessel. Suggest that this includes the status of Power Supply and Antenna Availability | | **Y** |
| | **Future Capabilities** | It is recommended that with the introduction of Level 2 Functionality that it be a requirement for new equipment (new models, etc) to have a capability to provide a status message to the LRIT ASP at regular intervals, or on demand, that indicates the 'health' of the equipment | | **TBA** |
| | **Time Stamp** | LRIT ASPs must be capable of accurately adding the following time stamps to LRIT data received from LRIT equipment:<br><br>a) The time (UTC) the report was received by the LRIT ASP, and<br><br>b) The time (UTC) the report was forwarded to the LRIT Data Centre | **Y** | **Y** |
| | **Interface with LRIT Data Centres** | LRIT ASPs must be capable of processing all prescribed configuration requests for LRIT data from LRIT Data Centres | **Y** | **Y** |
| | **Latency** | LRIT Data Centres must be capable of:<br><br>a) Transmitting LRIT data to LRIT Data Centres in "real time" following the receipt of LRIT Data from individual vessels [less than or equal to 1 minute], and<br><br>b) Responding to requests from LRIT Data Centres for LRIT data from vessels in "real time" [less than or equal to 1 minute] | **Y** | **Y** |

| Equipment / Provider | Parameter | Comments | Functionality | |
|---|---|---|---|---|
| | | | Level 1 | Level 2 |
| | **System Integrity** | LRIT ASPs must be capable of monitoring the integrity of LRIT data in terms of accuracy, reliability and latency. While such capability will assist to diagnose wilful attempts to compromise the validity of the data being transmitted it will provide invaluable diagnostic information LRIT ASPs, LRIT data Centres and contracting governments where there are genuine problems/faults | **Y** | **Y** |
| | **Positional Accuracy** | The positional data received by the LRIT ASP is to be monitored to detect a faulty GNSS unit on the equipment. | **Y** | **Y** |
| | **Time Stamp Accuracy** | The Time Stamps provided by both the equipment and the LRIT Equipment, LRIT ASP and the LRIT Data Centres must be monitored | **Y** | **Y** |
| | **System Availability** | <To Follow> | **Y** | **Y** |
| **LRIT DATA CENTRES** | **Configuration Capabilities** | LRIT Data Centre(s) must have the capability to request LRIT ASPs to remotely configure prescribed equipment to forward LRIT information as described in Section 4.2.3, irrespective of where a vessel is, and to subsequently receive LRIT information from that vessel irrespective of where it transits | **Y** | **Y** |
| | **Time Stamp** | LRIT Data Centre(s) must be capable of accurately adding the time (UTC) the LRIT report was received by the LRIT Data Centre and the time (UTC) the data report was forwarded from the LRIT Data Centre to the Contracting Government to each LRIT data report.<br><br>The LRIT Data Centre is also responsible for monitoring the validity of GNSS position (both the actual latitude/longitude and time stamp) received from Prescribed equipment and advising the contracting Governments accordingly. | **Y** | **Y** |
| | **Interface for Contracting Governments** | LRIT Data Centre(s) must be capable of receiving configuration requests for LRIT data from contracting governments in a standard, fixed format | **Y** | **Y** |
| | **Latency** | LRIT Data Centres must be capable of:<br><br>a) Transmitting LRIT data to contracting governments in "real time" following the receipt of the report from individual vessels [less than or equal to 1 minute], and<br><br>b) Responding to requests from Contracting Governments for LRIT data from LRIT ASPs in "real time" [less than or equal to 1 minute | **Y** | **Y** |
| | **System Availability** | <To Follow> | **Y** | **Y** |

**TASK 8: SYSTEM ARCHITECTURES**

## 1 Summary of MSC 80's conclusions and guidance to the Correspondence Group

Make recommendations on all system architectures that will meet LRIT performance requirements (potential service providers are encouraged to provide information in this regard);

## 2 Background material

a. IMSO MSC 80/5/5
b. Marshall Islands MSC 80/5/9
c. European Commission MSC 80/INF.2
d. Marshall Islands MSC 80/J/20
e. IMSO MSC 80/J/21
f. Final Report MSC 80/24 (paragraphs 5.67, 5.94 to 5.97 and 5.104)

## 3 Outline of the Correspondence Group's objectives as regards this task

The following paragraph presents the pertinent points of document MSC 80/24 (original paragraph numbering has been retained):

5.94 The Committee noted the deliberations of the Group with respect to architecture of the LRIT system and decided that the LRIT architecture should:

.1 enable the ship to transmit LRIT information to LRIT Tracking Services. A ship may use any approved LRIT Tracking Service acceptable to the ship's Administration. The system should allow for multiple LRIT Tracking Services (i.e. Application Service Providers) and Communications Service Providers. The LRIT Tracking Services should provide LRIT information to LRIT Data Centre(s). SOLAS Contracting Governments should be able to obtain LRIT information from LRIT Data Centre(s). The LRIT Co-ordinator should carry out oversight functions and should report its findings to the Organization;

.2 not allow a ship to transmit LRIT information directly to a port or a coastal State;

.3 allow for the interfacing with national vessel monitoring systems;

.4 not prevent the Administration from obtaining LRIT information from the national vessel monitoring system; and

.5 allow for varying the frequency of reporting.

Documents MSC 80/5/5, MSC 80/5/9, MSC 80/INF.2, MSC 80/J/20, MSC 80/J/21, and MSC/ISWG/LRIT 1/3/4 present a range of alternate LRIT solutions, both conceptual and actual. In reality, with the exception of a centralized/distributed issue, the system architectures are basically the same. Documents MSC 80/5/9 and MSC 80/J/20, both submitted by the Marshall Islands, provide a technically developed design rather than concept. The architecture remains largely unchanged from that originally proposed, however the associated discussion and diagrams have been updated to take into account the emerging task proposals from this Correspondence Group.

## A. Elements of the LRIT Architecture

The LRIT system includes all relevant hardware and software functions, including quality of service (QoS) monitoring facilities. The LRIT reports distributed to the various Contracting Governments should have a standardized format. The architecture is based upon the core functional and interface layers listed below and detailed in subsequent sections (associated correspondence group tasks are shown in brackets in the list, and in numbered boxes in the figure):

Functional Layers

- Shipboard Equipment (6, 9, 11)
- Communications Service Provider (6, 9, 11)
- Application Service Provider (13)
- National LRIT Data Centre
- International LRIT Data Centre (1, 2, 4, 5, 10)
- LRIT International Data Network
- LRIT Co-ordinator/IMO

Interface Layers

- Flag, Port, and Coastal States (14)
- Search and Rescue (SAR) (12)

### I. Shipboard Equipment

The following existing shipboard equipment may meet LRIT requirements:

**SOLAS IV GMDSS** – Many shipping companies using commercial LRIT 'Application Service Providers' (ASPs) use existing GMDSS equipment, which has near-global coverage and provides, two-way and automatic position reporting (APR) in near-real-time.

**SOLAS XI-2/6** requires carriage of a ship security alert system (SSAS) for vessels engaged on international voyages. The SSAS is generally GNSS-equipped and may be used by SSAS ASPs to offer value-added tracking services. Consequently, this equipment could be used for LRIT purposes. Given SSAS performance variations, it is recommended this equipment meet the minimum LRIT performance standard established by the IMO. Furthermore, in order to protect disclosure of shipowner/Flag State SSAS operations, there should be a clear functional, routing and accounting separation of SSAS security alert reporting and LRIT-specific information (i.e., any alert information should not form part of the LRIT information package).

**Non-SOLAS** – integration of non-SOLAS based technologies and tracking techniques (e.g., fleet management systems) which meet LRIT performance standards should also be considered. The shipboard equipment should:

- Operate in Automatic Position Reporting mode to avoid shipboard personnel intervention
- Operate using shore-based on demand position reporting and dynamic APR interval modification
- Operate using a tamper evident reporting logic (or alternately by the shore-based application)
- Operate using an integrated GNSS
- Be type approved to the relevant marine equipment standards.

## II. Communications Service Provider (CSP)

Commercial CSP's operate using proprietary communications protocols unique to the service provider. LRIT information security is achieved using these proprietary protocols, as opposed to the use of encryption protocols (as applied by the military). Although specific terminology may change, CSPs operate using almost identical architectures; shipboard terminals, satellites (as appropriate), earth stations, and message handling systems. CSPs may be satellite or terrestrial-based systems operating in a variety of frequency bands. In some cases, a CSP may act as its own Application Service Provider (ASP).

The CSP should:

- Operate in accordance with coverage specified in SOLAS IV.
- Operate using a secure point-to-point communications protocol, precluding non-secure broadcast systems.
- Be responsible for ensuring data is transferred to the ASP in a secure manner.

## III. Application Service Provider (ASP)

ASP's can be categorized as either single-service or multi-service. Single-service ASPs offer services dedicated to one specific CSP, while multi-service ASPs offer services using multiple CSPs. An LRIT data centre could be operated as a multi-service ASP.

When operating with an International Data Centre, National LRIT Data Centre, or ASP, Contracting Governments would have at their disposal several methods of interfacing with an LRIT data centre, including:

- Web application interface (requires an internet-enabled computer),
- Local specialized client (requires dedicated PC-based workstation product),

Contracting Governments could select their preferred interface method from the web application interface and local specialized client offered by the LRIT Data Centre operators or ASP. In this way, Contracting Governments having zero or very little established capability could have equal access to LRIT information as do Contracting Governments that have already established national monitoring capabilities.

## IV. National LRIT Data Centre

Some Contracting Governments already operating tracking services for their national fleets may prefer not to transfer data concerning their fleets to an International LRIT Data Centre. In this case, a National LRIT Data Centre may respond to requests for data on their ships from their repository directly to the requestor based on their Port State, Coastal State, SAR or environmental protection status. National LRIT Data Centres should be able to meet the same performance requirements (latency, etc.) as the LRIT International Data Centre. Any additional costs associated with modernization of an existing National LRIT Data Centre should be borne by the Contracting Government operating the centre.

Every National LRIT Data Centre should have at least two copies of LRIT database. The National LRIT Data Centre should be connected to two different Internet Service Providers (ISP). The LRIT National Data Centre should have the facilities to send poll commands to the

flag vessels directly or indirectly. Every National LRIT Data Centre has to interact with National LRIT Data Centres of other Contracting Governments. Contracting governments can create collective National LRIT Data Centres.

Data security – Each flag State, port State, coast State and other entities interested in and authorized to have access to LRIT data should all have individual IMO-signed digital certificates to access LRIT data centre(s) to receive information, to define and change the settings and various parameters related to all ships they are granted access, including polling requests for individual vessels or group of vessels. Digital certificates will securely authenticate the user while giving IMO control over access to the LRIT system. Two-factor authentication (e.g., electronic token) could also be considered to ensure the identity of the entity accessing the data. While authentication and authorization will typically take place over the Internet, other links such as PSTN could also be possible. In this respect, attention should be paid to the use of a bandwidth efficient protocol as connection bandwidth may be limited in some locations.

Archiving LRIT information – National LRIT Data Centres should be capable of archiving LRIT information.

It will be necessary for the National LRIT Data Centre to regularly update its database to verify ship flag and other data. Communication links must therefore exist between the National LRIT Data Centre and national ship documentation centres.

## V. LRIT International Data Centre

The International LRIT Data Centre can be created as the central point of data interchange which will have data about fleets of all Contracting Governments. The LRIT International Data Centre should consist of a real or virtual main database with a back-up database in a separate location. The two databases should have separate terrestrial links to all interfacing equipment and a leased line interconnection for synchronization and replication of data. The LRIT reports from the ships should be sent directly from the ASPs to the LRIT Data Centre (main and back-up databases) using separate internet, leased lines or PSTN depending on the facilities and preferences of the various satellite earth stations. The communication links between the LRIT databases and ASPs. The International LRIT Data Centre can be created as the central point of data interchange. The central point will have data about fleets of all the Contracting Governments.

Data security – Each flag State, port State, coast State and other entities interested in and authorized to have access to LRIT data should all have individual IMO-signed digital certificates to access the International LRIT Data Centre(s) to receive information, to define and change the settings and various parameters related to all ships they are granted access, including polling requests for individual vessels or group of vessels. Digital certificates will securely authenticate the user while giving IMO control over access to the LRIT system. Two-factor authentication (e.g., electronic token) could also be considered to ensure the identity of the entity accessing the data. While authentication and authorization will typically take place over the Internet, other links such as PSTN could also be possible. In this respect, attention should be paid to the use of a bandwidth efficient protocol as connection bandwidth may be limited in some locations.

Archiving LRIT information –LRIT International Data Centre should be capable of archiving LRIT information.

## VI. LRIT International Data Network

The LRIT System could consist of a number of National LRIT Data Centres or an International LRIT Data Centre. LRIT data exchange may be organized:

- Through a central point (centralized system)
- On the "end-to-end" principle (distributed system)

For both variants, the Internet should to be used as the core of the network. IMO and Contracting Governments should agree on the principle of an LRIT International Data Network.

Management and control – Regardless of how data is exchanged, (centralized or distributed), control and security of the LRIT system should be effected through the use of a Public Key Infrastructure (PKI), securing connections via a certificate based protocol (e.g. Transport Layer Security – TLS – protocol) and automated certificate management (e.g., via the Online Certificate Status Protocol – OCSP).

Data security – Security of the data is a fundamental requirement for the LRIT system and must be a key part of its design. The introduction of the International Data Centre between ASP and User may reduce the security of data that would otherwise remain encrypted and delivered to a duly authorized recipient. Information from National LRIT Data Centres is not subject to this security problem as information is drawn directly from their repositories. All National LRIT Data Centres should use the same algorithm to organize Virtual Private Network (VPN) channels or establish secure connections for data interchange.

To tune every National LRIT Data Centre to interoperate over the LRIT International Data Network, demo National LRIT Data Centres (performing only data exchange) could be created and installed for free testing of secure interconnection and/or VPN functionality. It will be necessary for the International LRIT Data Centre to occasionally verify ship flag and other data. Secured communication must therefore be possible between the LRIT Data Centres and national ship documentation centres

## VII. LRIT Co-ordinator/IMO

The Group agreed that an LRIT Co-ordinator may be needed for oversight of the performance of LRIT communications and application service providers. However, it was also agreed that the oversight organization should not be involved in running commercial data services such as the international LRIT Data Centre. The LRIT co-ordinator could be appointed by IMO (MSC) similar to the NAVTEX Co-ordinator. The LRIT co-ordinator should provide regular reports to IMO (MSC/COMSAR) on the performance of the international and national LRIT Data Centre(s). Intersessionally, an IMO LRIT Panel could keep an updated register of national LRIT requirements as declared by Governments and a list of national LRIT VMS. The LRIT co-ordinator and oversight functions are distinct and could be accomplished by different bodies.

The LRIT Co-ordinator may also be called upon by IMO to assist in establishing the LRIT data centre, for example:

- Define/specify the complete requirements for LRIT Data Centre(s)
- Issue the tender/Request For Proposal on behalf of IMO
- Evaluate the management, technical, and financial proposals
- Issue/manage the subsequent contract (for a duration to be determined by IMO)

## B. Alternative: Centralized Architecture

In this alternative of the LRIT system architecture, data is exchanged through a central point – the LRIT International Data Centre. The LRIT International Data Centre will keep all the information about fleets of the Contracting Governments.

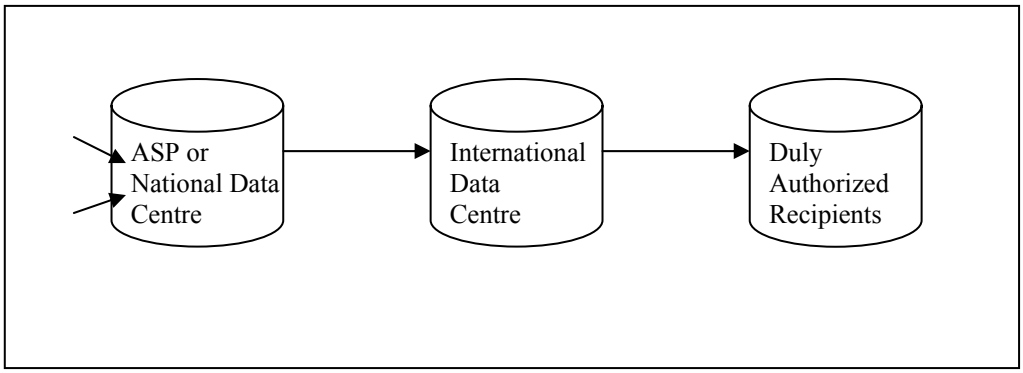


**Figure 1. Centralized Architecture Concept**

Figure 2 presents the details of a centralized LRIT architecture. In some cases, a CSP may act as its own Application Service Provider (ASP) and will interface directly with the LRIT international data network. This scenario is reflected in the architecture diagram by the single arrow entering the top of the LRIT international data network.

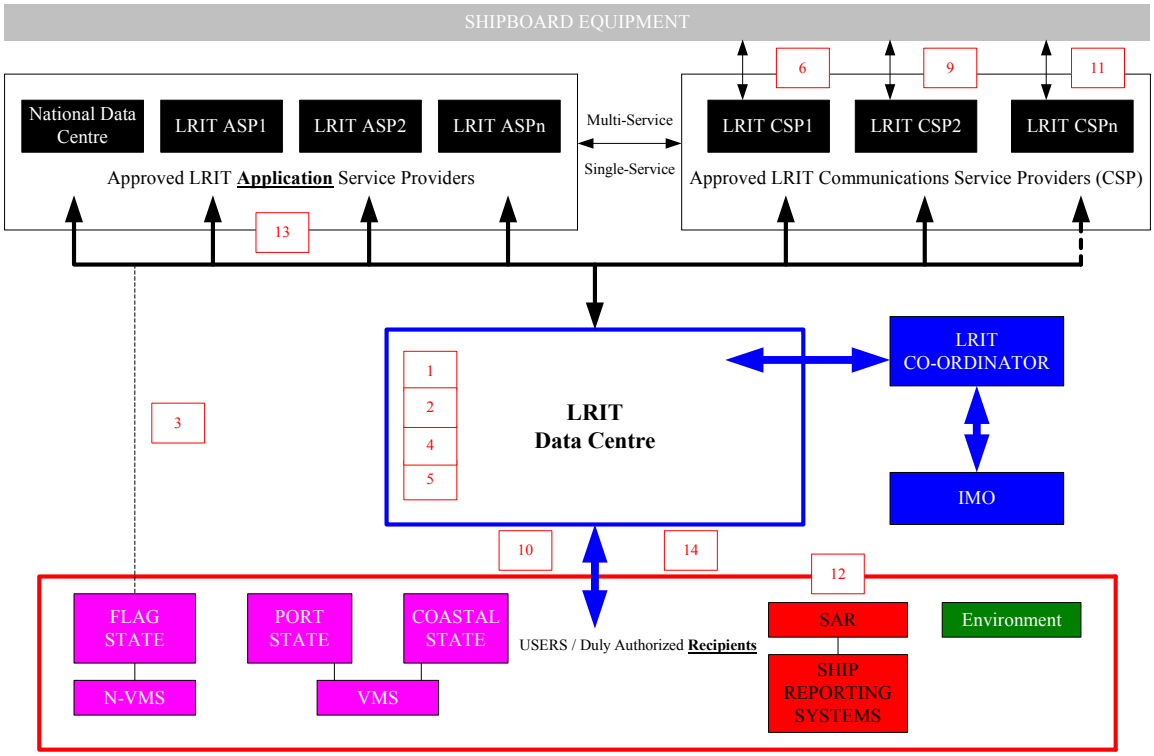


**Figure 2. Centralized LRIT Architecture**

## C Alternative: Distributed Architecture

In the alternative of a distributed LRIT architecture, there is no centralized database. The concept diagram of a distributed architecture is shown in Figure 3.

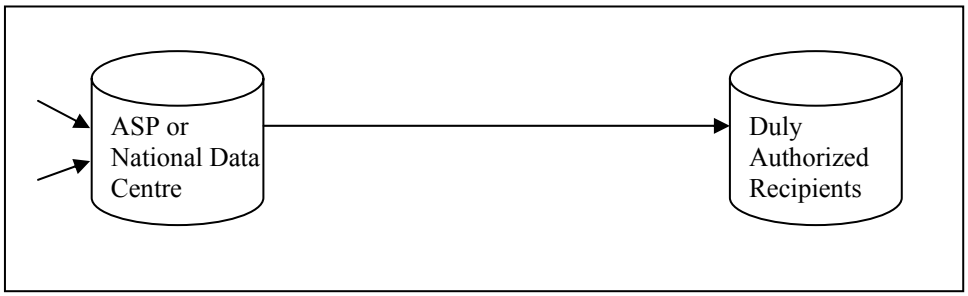


**Figure 3. Distributed Architecture Concept**

Figure 4 presents the details of a distributed LRIT architecture. In this approach, multiple national or regional LRIT Data Centres exchange information without the need of a centralized database. Each National Data Centre will get LRIT information about its flag vessels and vessels of other Contracting Governments to which it has been granted access. However, for MRCC requests, a special centre can be created. It is not in fact a database, but rather an "agent" that can accept the request for data collection for SAR operation from one of the National LRIT Data Centres and request other National LRIT Data Centres for vessel positions in the area of a SAR case.

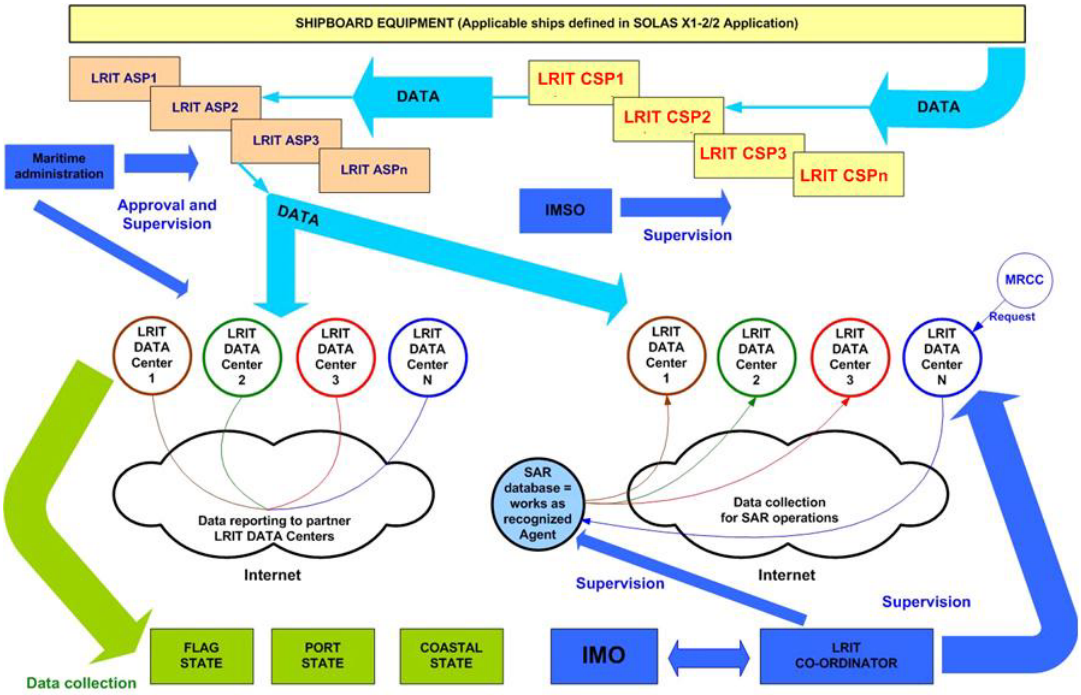


**Figure 4. Distributed LRIT Architecture**

Information about fleet disposition is sensitive from both a commercial and security perspective. Contracting Governments may not wish to allow the distribution of such information through an international data centre (as opposed to each Administration individually controlling release of LRIT information on its Flag's ships).

Contracting Governments should have enough flexibility to implement a structure which is acceptable for national regulations while meeting IMO LRIT requirements. With regard to vessel monitoring systems (VMS) to conduct LRIT operations, an Administration could approve one or more of the LRIT services whose performance is not inferior to IMO requirements. An Administration could appoint a national LRIT ASP that would function as a national data centre and would interface with the LRIT Data Centre(s). It is possible that some Administrations will group into regional vessel monitoring systems for this purpose or they may select an international ASP from current commercial companies. Those national LRIT ASPs could establish commercial relations with governments who appoint them to provide services. This flexibility will allow sensitive data to be secured from source (VMS) to destination (user) and incorporate innovative new technologies.

## D. Hybrid Architecture for SAR

Using this hybrid architecture, a centralized SAR database (or agent server) could serve as an international tool to help any MRCC during SAR operations, as shown in Figure 5.

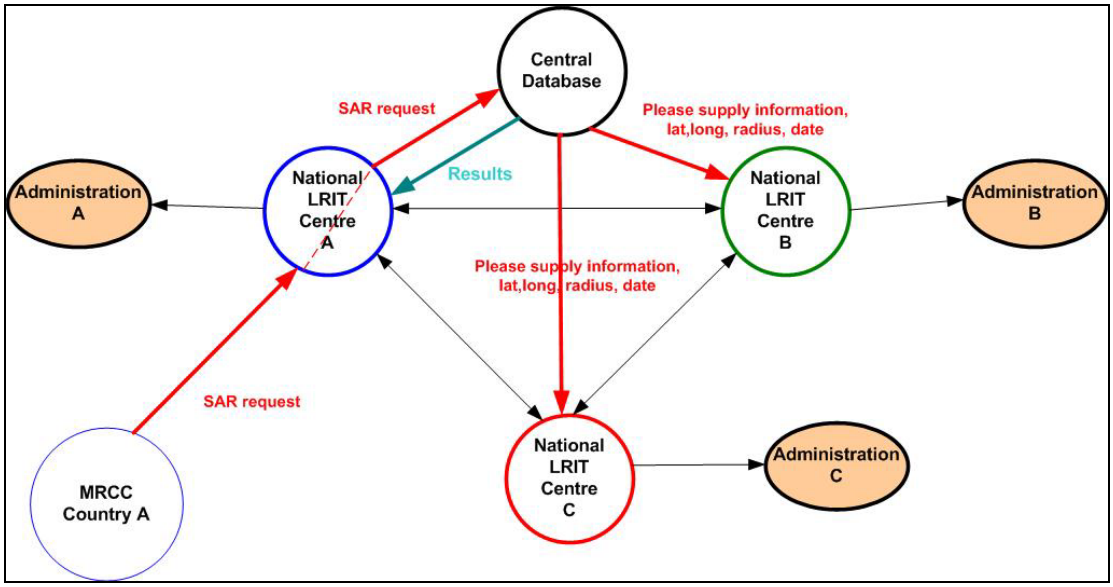


**Figure 5. Hybrid LRIT Architecture for SAR**

In this instance, the system can be considered as de-centralized for day-to-day operation and being centralized for short times in certain ocean areas for SAR operations. This approach could also be applied as overall LRIT architecture allowing a mix of centralized and distributed architecture to facilitate early implementation of LRIT.

## E. Conclusion

Most members of the Group preferred a centralized architecture. However the need to respect national regulations and other information security concerns may give credence to a distributed architecture. Some Contracting Governments may wish to retain direct control over the LRIT information on those ships flying their flag and this could influence how they interact with the national and international LRIT Data Centres.

New technologies continue to emerge that may drive changes in the architecture to enhance security, increase functionality and reduce costs. SOLAS amendments and associated functional specifications should not specify a particular architecture and should remain flexible when it comes to ensuring the security and safety of mariners.

## TASK 9: VARIABLE LRIT REPORTING RATES

### 1 Summary of COMSAR 9's conclusions and guidance to the Correspondence Group

Make recommendations regarding the ability of Contracting Governments to vary the LRIT information reporting rate from ships

### 2 Background material

Variation in reporting rates has already been agreed as a requirement for LRIT architecture by MSC 80 (MSC 80/WP.7/Add.1, paragraph 5.5 and MSC 80/WP.6/Add.3, paragraph 5.74.5).

The Committee decided (in MSC 80/WP.6/Add.3 paragraph 5.74) that the LRIT Architecture should: …

.5 allow for varying the frequency of reporting.

The possibility of obtaining reports from all ships within specific geographical limits was also discussed during MSC 80 under the provisional name of "pinging" (MSC 80/WP.7/Add.1, paragraph 25).

### 3 Correspondence Group's response

*Varying Security Levels*

The principle of LRIT is to allow tracking of ships via position reporting. Varying the frequency of reporting from ships can provide vessel positions at sufficiently regular intervals that are relevant to security levels and to vessels' distance from ports or coasts. Higher reporting rates will provide better track granularity. The number of position reports could be varied according to the type of vessel (based on security levels) or by the position of the ship at sea.

Under security level 1 and/or when ships are at considerable distances [>300 miles] from coasts, LRIT reporting rates can be very low – perhaps as low as once per day. At higher security levels, and particularly at Level 3 or when ships are nearer to ports or coasts, reporting rates need to be more frequent.

*Cost optimization*

Variable LRIT reporting rates can offer direct control of LRIT costs. By controlling the frequency of ship reports, LRIT communications costs can be optimized to match the security requirements of Administrations. Costs can be optimized based on regular position reports along the ship's route, with additional more frequent polls on demand or by increasing the regular reporting rate. For maritime security, the frequency of the ship's reporting rate needs to be variable or, if fixed, sufficient to satisfy the most frequent reporting rate.

Recognizing that course and speed must be derived from successive position reports, shorter intervals will provide better estimates of course and speed. Accordingly, a minimum frequency of [4] reports per day is deemed necessary.

Ships in ports are in a special situation. Since the ship is within the [300] nm boundary (as noted in draft SOLAS text), it will therefore be programmed to send at the most frequent interval (if a Contracting Government is interested in the ship's movements). All satellite transceivers with the possibility of internally analyzing movement should be programmed to only send position reports every [24] hours when not moving, and to send the first position report as soon as possible after moving a distance of at least [2] nm. To avoid the LRIT Data Centre from sending an automatic poll to vessels in port, the LRIT Report should be enhanced to include an "in port" flag that could be true or false. This "port flag" is a requirement placed on the LRIT Data Centre to incorporate and should not revert to the polled ship for any required action.

*On demand LRIT reporting within geographic limits*

Consideration should also to be given to the desirability of obtaining LRIT reports on demand for all ship/s within specific geographic limits e.g. within a certain specified distance of a port, vessel, or suspected incident.

By having the ability to control the frequency at which ships report and by obtaining reports on demand, a current "surface picture" be obtained and maintained as a necessary element of LRIT.

This was also discussed during MSC 80 under the provisional name of "pinging" (MSC 80/WP.7/Add.1, paragraph 25) as a possible future enhancement for LRIT.

## TASK 10: LRIT DATA CENTRE LIST OF SHIPS

### 1 Summary of MSC 80's conclusions and guidance to the Correspondence Group

Consider the practical issues associated with the maintenance by the LRIT Data Centre of an up-to-date list of ships which are required to comply with the SOLAS regulation on LRIT.

### 2 Background material

MSC 80/WP.7/Add.1, paragraph 7

### 3 Correspondence Group's response

*Background*

The LRIT Data Centre will be required to hold a list of ships to which the LRIT SOLAS regulation applies. Based upon the Flag of each ship a range of data access rules pertaining to Flag, Port and Coastal State usage will be applied. This will require that all data associated with LRIT compliance is stored for each ship, and is as up to date as possible.

The report of the maritime Security Working Group (MSC 80/WP.7/Add 1), invited the Committee to decide that each Administration should be required, before the SOLAS regulation on LRIT enters into force, to provide the LRIT Data Centre with information about the ships entitled to fly its flag which are required to transmit LRIT information, and thereafter to promptly advise the LRIT Data Centre of any relevant changes.

*Discussion*

When a ship enters or leaves a Flag, as part of the transfer process there is a de-commissioning and re-commissioning of GMDSS and other communications arrangements – upon completion this is an indicator to the Administration concerned that Flag change is technically accomplished. Furthermore, it must be expected that ship's name, Flag designation, Primary and Secondary LRIT system identifiers/serial numbers and LRIT active/inactive status could change with a change of ownership and management.

For the LRIT Data Centre set-up, the following basic parameters will be required from each Flag for each ship in the form of an "LRIT-FS Initial Set-Up Report" (FS=Flag State):

1. Ship's Registered Name
2. IMO Number
3. Call Sign
4. MMSI
5. Primary LRIT system identifier/serial number
6. Secondary LRIT system identifier/serial number (optional)
7. LRIT active/inactive
8. Company Security Officer (CSO) name and contact details

- Parameter 1 is the registered name of the ship.
- Parameter 2 – is the ship IMO number which is recommended be utilized as the database primary key i.e. the unique identifier that distinguishes a ship from all others (given that it is common for multiples of the same ship name to be in use and for the call signs/MMSI to change).
- Parameter 3 is the ship Call Sign as assigned by the national licensing authority, the first one to three characters identifies the ship's flag under ITU convention.
- Parameter 4 is the ship MMSI, a series of nine digits which uniquely identifies the ship's flag, ship station, ship earth station, coast station, coast earth station, and group calls.
- Parameter 5 is the Inmarsat C mobile number (for example) and serial number of the associated terminal – a combination of the two allows ownership validation and so adds an extra layer of security.
- Parameter 6 (optional) provides a backup LRIT system in the event of failure/problems with the primary system. This may be an SSAS type or dedicated system.
- Parameter 7 specifies if an LRIT system is active or inactive from the point of view of Flag State operation (a Flag may choose not to track its ships).
- Parameter 8 is the Company Security Officer and contact details (*a secure on-line procedure could be established to allow the CSO to input/update information in this respect).

In the event a ship changes flag the following parameters will be required from the outgoing Flag for each ship in the form of an "LRIT-FS De-commissioning Report":

*Outgoing Flag*

1. IMO Number
2. Date/Time of De-commissioning

In the event a ship changes flag the following parameters will be required from the incoming Flag for each ship in the form of an "LRIT-FS Commissioning Report":

*Incoming Flag*

1. Ship's Registered Name
2. IMO Number
3. Call Sign
4. MMSI
5. Primary LRIT system identifier/serial number
6. Secondary LRIT system identifier/serial number (optional)
7. LRIT active/inactive
8. Date/Time of Commissioning

It is anticipated that the LRIT-FS De-commissioning and Commissioning statements would be received by the LRIT Data Centre in close duration to each other. In the event that either one of the reports is received in isolation of the other, the applicable report will be placed in a 'temporary holding area' awaiting receipt of, and cross reference with, the associated report. A time threshold will have to be placed on the duration of this holding period, and the action to take be determined in the event that an associated report is not received.

## TASK 11: ADDITIONAL LRIT INFORMATION

### 1 Summary of MSC 80's conclusions and guidance to the Correspondence Group

Ensure that the ship should not be required to transmit to the LRIT Tracking Service or the LRIT Data Centre, any additional information (except the transmission of a notice that the ship is proceeding to a particular port, to enable the LRIT Data Centre to provide the Port State with the LRIT information to which it is entitled) and that the transmission of LRIT information should not require any intervention by shipboard personnel.

### 2 Background material

MSC 80/WP.7/Add.1 paragraph 10

### 3 Correspondence Group's response

IMO discussion has agreed that the composition of the LRIT data package required of SOLAS ships is:

- Unique ship identity
- Time of report
- Position

The factors that have resulted in this decision are the need to keep transmission costs as low as possible and the total of LRIT data to a manageable level. This decision was re-affirmed at the MSC intersessional meeting (17 to19 October 2005).

[To make the future system with transmission costs as low as possible, regular data reports should be made with the frequency of data reporting acceptable for most Contracting Governments.]

It is impossible accurately to predict the number of SOLAS ships at sea at any one time but perhaps a figure of around 50,000 could be considered a working figure. On the assumption that authorities using LRIT for security purposes will be automatically plotting LRIT data and that a reasonable frequency of reporting will be established, the IMO decision on the data package facilitates a workable picture compilation system. Too much data may tend to conceal the really important information amongst a mass of reports on legitimate trading movements.

In the context of security, the less that the crew are required to interact with the system in terms of inputting data, the more secure the system can be considered. There has been some discussion of the need for an outline voyage plan to be submitted by the ship on sailing. Experience already with AIS has shown that voyage specific data is not routinely updated in a significant number of ships. In the case of LRIT where the ship will not be aware of the transmitted information it seems logical to expect that voyage related data may also be forgotten or incorrectly input. The regular plotting of the basic LRIT data package makes the prior notification of voyage data unnecessary and may be a hindrance rather than a help to security organizations. In the case of an ill-intentioned crew who may wish to conceal or falsify voyage information it is preferable that no crew interaction with LRIT should be possible.

Discussion at MSC 80 revealed that political considerations of the ranges at which port and coastal States might be authorized to receive LRIT data could have an impact on the data required of ships. There is a particular problem with port States where the current intention is to permit the port State access to tracking information on any ship that has declared the intention to enter a port in its jurisdiction. This raises a question on how this may be ascertained. In the case of some states, there is already a requirement to transmit a notice of arrival message at a set period before arrival. There is no reason why this could not be forwarded by the port State to the LRIT oversight body to trigger the flow of data.

It is also possible that the LRIT Data Centre and/or ASPs may offer an advance notice of arrival (ANOA) service. Such a service would require the provider to maintain a database of the appropriate points of contact in port States which require ANOAs. The provider would relay ANOAs from client ships to the port State points of contact. If provider is an ASP rather than the LRIT Data Centre, the Data Centre would also receive the ANOA. The Data Centre would then know which States are entitled to receive port State reports. Such an arrangement has several benefits for the ship: 1) there would be no need for the ship to separately authorize the LRIT Data Centre to provide reports to a unconfirmed port State; 2) the ship would not need to maintain current listings of ANOA points of contact; and 3) there would be no need for the ship to determine which port States require ANOAs, if it routinely informs its ASP of all scheduled ports of call.

The LRIT Data Centre may request the Port State for evidence of the legitimacy for requesting LRIT Information, such as Advanced Notice of Arrival, when the LRIT Data Centre needs to confirm it.

Giving Port States access to the relevant LRIT reports should be handled automatically by the LRIT Data Centre. The notice that the ship is proceeding to a particular port needs to be formatted according to a predefined message to enable the LRIT Data Centre to automatically process the information and set up the proper access parameters for the Port State named in the notice.

One potential process for validating Port State access to LRIT data follows:

1. Port State receives an ANOA/or equivalent as per national requirement (X hours out of port/or Y nautical miles distance).

2. Port State submits a Port Integration Request (PIR) to the LRIT Data Centre for tracking of ship between start date/time and end date/time.

The notice that a ship is proceeding to a particular port will not necessarily give any indication to the LRIT Data Centre about the Coastal State "boundaries" (i.e., a line offshore that marks the distance that a Coastal State wishes to obtain LRIT information) which the ship may cross during its navigation. Having a database for all such distances of all Contracting Governments, the LRIT Data Centre(s) could start the supply of information to the Coastal State(s) automatically. A Contracting Government could agree to define the distance offshore for which it requires LRIT information. This will allow the LRIT Data Centre(s) to start the supply of information automatically using regular LRIT information reports to the LRIT Data Centre or national VMS.

Some vessel data reports (e.g., Ship Reporting Systems, VMS, fleet management systems) also include course and speed. For communications systems that automatically provide for transmission of course and speed at no additional cost per message, the LRIT System should be capable of utilizing this additional information and it should be provided to the authorized Contracting Government requesting it.

It should also be borne in mind that under the amendment to SOLAS Regulation V/28 and with effect from 1 July 2006 all ships of 500 gross tonnage and above, engaged on international voyages exceeding 48 hours, are required to submit a daily report to their company, to include ship's position; ship's course and speed; and details of any external or internal conditions that are affecting the ship's voyage or the normal safe operation of the ship. It does not seem coherent to apply another separate requirement for the transmission of a message indicating the next planned port of call. There is merit in examining this pre-existing requirement to look for a synergy that may be established with LRIT.

There has been discussion on the use of LRIT data for purposes in addition to maritime security such as for pollution prevention and SAR. Even in these cases, it is hard to justify the additional expense and increase in the volume of data that would be required to provide more ship or voyage related information. In any tracking system, for any purpose, the basic information of identity, time code and position provide sufficient information to locate the ship, to predict its expected movement, to concentrate other tracking assets or if necessary to contact the ship. The potential for pollution prevention provides a strong argument for the retention of historic LRIT data at the service provider or tracking facility.

Ships engaged in international trade are subject to commercial operational influences which must be taken into account when considering additional information for LRIT. Often a ship will sail from the loading port with no clear knowledge of the intended next port of call and this is particularly relevant in the tanker and bulk carrier trades. Likewise the next port of call may be changed more than once during the voyage in response to commercial decisions. It is therefore considered that the transmission of a voyage plan, containing both nugatory and time-sensitive information may place an unnecessary burden on the tracking organizations. It appears to be more appropriate to require the minimum amount of data to be transmitted from the ship. Any data transmitted by the ship in support of the LRIT requirement must be accorded the same degree of protection as the core data package.

It is concluded that, the data package for automatic LRIT transmissions should be confined to ship identity, position and time. Any supplementary information could be derived from the existing SOLAS position report by simply adding an appropriate LRIT addressee to the message.

The system should be automatic without need of any crew interaction with the shipboard equipment. Furthermore, manual data input by LRIT Data Centre(s) and LRIT service provider personnel should be minimized. Therefore, the system should work without notices generated by ships or Port Authorities.

## TASK 12: RCC USE OF LRIT INFORMATION FOR SAR

### 1 Summary of MSC 80's conclusions and guidance to the Correspondence Group

Consider the Committee's decision that LRIT information for search and rescue (SAR) purposes should be provided free of charge to the Rescue Co-ordination Centre (RCC) co-ordinating the performance of SAR operations and/or to the SOLAS Contracting Government in which the RCC is located. If necessary, develop appropriate arrangements taking into account the provisions of resolution A.707(17) on Charges for distress, urgency and safety messages through the Inmarsat system.

### 2 Background material

MSC 80/WP.7/Add.1, paragraph 21

### 3 Correspondence Group's response

LRIT data should be:

a. Available to rescue co-ordination centres (RCCs) on request via a single global point of contact.

b. Provided solely to RCCs recognized by IMO and/or the International Civil Aviation Organization (ICAO), and solely for responding to an actual or apparent incident of maritime or aeronautical distress at sea.

c. Maintained or archived for four days, because historical data help in situations with ships where communications have been lost or that are overdue, or in identifying ships that were in the vicinity of a distress situation that may have heard or seen something relevant. (Also applies to Task 4).

d. Available for areas outside an RCC's own SAR region, as an RCC often needs to co-ordinate SAR in such areas in the role of "first RCC" to receive an alert, or when the RCC is best situated to respond.

e. Be provided to RCCs electronically and in a standard format so it can be automatically plotted when received.

IMO should work with ICAO to promulgate appropriate guidance to aeronautical and joint (aeronautical and maritime) RCCs on access to and use of LRIT data for SAR.

## TASK 13: COST OF LRIT INFORMATION VS. AVAILABLE TECHNOLOGIES

### 1 Summary of MSC 80's conclusions and guidance to the Correspondence Group

Consider, in an effort to minimize the cost of the initial establishment of the LRIT system, and the LRIT information charges, all possible forms of technology. However, these should not require ships to fit additional or new equipment on board, recognizing that ships may require appropriate software and that ships operating in Sea Areas A1 and A2 may need to fit additional equipment.

### 2 Background material

MSC 80/WP.7/Add.1, paragraphs 22 to 27
COMSAR 9/WP.5/Rev.1, annex 1, paragraph 6.5 (Draft SOLAS Amendment, provided as annex C of LRIT C/G Work Plan), as follows:

> 6 Contracting Governments shall, at all times:
>
> .5 cover all communication cost associated with the provision to them of any LRIT information they have requested to receive and shall ensure that information is provided at no cost, whatsoever, to the ship concerned.

### 3 Correspondence Group's response

*Discussion*

The benefits of an LRIT system may have several components, including increased safety and security and improved response times in case of emergency or piracy. Administrations have expressed an interest in the cost of LRIT information for all of the available technologies. The intent with regard to this Task is to address the operating cost to the Contracting Government, for available LRIT technologies. That is, such potential available technologies "should not require ships to fit additional or new equipment..." (MSC 80/WP.7/Add.1, paragraphs 22 to 27).

Accordingly, this Task focuses on systems using existing ship-fitted equipment (either mandatory, e.g., GMDSS or SSAS equipment, or optional, e.g., fleet management systems, etc.) that can accomplish LRIT functions. From these examples, estimates of operating costs are given in a variety of potential units, e.g., per ship/year, per message, per ton/year, or per time period, etc. This Task is central to gaining broad international acceptance for implementation of an LRIT system(s).

*Existing Technologies*

Long Range Identification and Tracking will be facilitated by the availability of multiple commercial satellite systems; the aggregate coverage of such systems is global, and the commercial functionality permits the addition of a simple data service for LRIT. In this respect, there are no direct alternatives to the proposed LRIT technology. Some existing technologies provide partial functional alternatives, such as AIS, shore-based radar, shipboard radar, VHF/UHF voice reporting. However, even when combined, these systems are clearly not capable of providing the global tracking required of LRIT.

The provision of dependable communication network(s) capable of continuous (and virtually instantaneous) global tracking is currently possible only using modern commercial satellite and also some terrestrial communications networks.

Although the costs of LRIT have not been fully determined, general estimates can be made using current commercial charges as a basis.

When considering costs, it is also important to note that an LRIT system can be set up immediately. It is possible that more advanced functionality for LRIT could be achieved by installing new software on existing equipment. This virtually non-existent lead-time represents a cost savings to Administrations and users alike.

LRIT should not impose additional new fittings. However, new technologies may be developed that will be less expensive in the long term. In telecommunications technologies, everyone has experienced (i.e. mobile phones, hi speed Internet, voice on Internet, etc) that the cost of hardware is balanced by the cost of operations after one year or two. Shipping companies are well aware of this, and many of them have invested in specific satellite communications systems for fleet tracking systems.

In addition, a large part of the LRIT costs will be fixed because of the dedicated infrastructure and not proportional to the number of reports. So it may be helpful to separate the investment costs, the recurring costs, and additional costs if any. That is, there should be a fixed charge to cover the development and operational costs of the LRIT system, and a variable charge depending on the actual number of LRIT reports received. This indicates that all authorized entities wanting to receive LRIT Reports will have to contribute to the development and operational costs in addition to pay for the actual reports received.

In order to assess the costs of LRIT operations, the flag, coastal and port States should propose scenarios for their future operations, to allow companies acting as Application Service Providers (ASPs) to evaluate the traffic (satellite and networks) and the data management. Because Administrations may not have flexible budgets, they will likely “auto-limit” their use of LRIT to control costs.

Collecting regular positions reports over a large number of ships may cost less than collecting “on demand positions” (i.e. polling) at frequent intervals. One poll may cost nearly as much as 10 automatic position reports in some systems. If ships have not reported before they enter into coastal waters, the Coastal State might send 3 or 4 polls to evaluate the ship route and speed. This could quickly deplete the “daily LRIT budget” for a Contracting Government on a given ship.

On the other hand, collecting regular reports every day from a large number of ships will create a body of knowledge of the ship routes and this will serve to feed a central database. If these reports are paid by the Flag States to track their Flag’s fleet, the cost is offset by Port and Coastal States requesting LRIT information. Once the data is collected and stored in the ASP database, the cost to access it by the port or coastal State is marginal (no satellite communications are required, since the data is already available, with only an access right paid to the ASP). If a Contracting Government asks for more reports (on demand positions), it must pay for them.

**Example**

Although the costs of LRIT have not been fully determined, a broad estimate can be made using current commercial charges as a basis: The following example has been suggested by a company which provides vessel-tracking services on a commercial basis at present.

*Equipment Cost:*

The current commercial service can be provided using existing equipment (e.g., GMDSS or fleet management systems). If already installed, there is no extra charge for equipment. If new equipment has to be installed, the cost ranges from US$1,500 to US$2,500. The upgrading cost will be paid by the shipping companies so as not to increase LRIT operational (recurring) costs.

*Cost of Reporting:*

Assume a single ship, making a ten-day trans-Atlantic voyage: *(assuming 50¢/report)*

| | |
|---|---|
| 8 days with four automatic reports per day: | US$16.00 |
| 2 days with 24 on-demand reports per day: | US$24.00 |
| Total cost of reporting during the ten-day voyage: | US$40.00 |

Generally, factors affecting the cost of reports will include the charges levied by the communications service provider (i.e., satellite operator) for carrying the message, a levy to cover the establishment and operating costs of the LRIT Data Centre and a levy to cover the cost of LRIT oversight.

The operating cost of LRIT is to be shared between the Flag, Port, and Coastal States. One can assume that the Flag State will pay for the regular daily positions, while the Port and Coastal State will request (and pay for) more frequent on-demand positions.

One Contracting Government (a large Port State) indicates that on an average day, 1,040 ships over 300 GT approach its ports from foreign ports carrying goods and passengers, with another 350 present within those ports. Overall, including coastwise traffic of foreign flag ships not bound for this Government's ports, an estimated 5000 of these ships are within 2000 NM of this Contracting Government at any time.

Increasing the information sent within a message will induce a higher cost of the message. Providing only essential information (Ship's identification, position, date/time) will optimize and reduce the cost of the message.

**Another example**

One HF-based communications provider offers its version of LRIT for as low as USD 6.00 per month per vessel. This rate provides an updated position every two hours.

**A Third Example**

The cost for only basic reports with 6 hours intervals (without the need for polling) will have the following estimate:

*Assumptions:*

The number of ships to be tracked is 40,000 (SOLAS ships) and the average cost per LRIT report is USD 0.05. The number of states and entities that would like access to the LRIT database (and therefore will have to share the costs) is 100.

The resulting cost per Contracting Government for the basic daily 4 reports will per year be: 40,000 * 0.05 *4*365 / 100 = USD 29,200. (or $2.9 M/year if not shared). Clearly, this cost is linearly proportional to the per message charge.

**A Final Example**

One Contracting Government has estimated that LRIT operations can be operated using an ASP at a "fleet-wide" cost of USD 0.003/GRT. This estimate was based on the number of this Contracting Government's ships that would have to participate in LRIT and their related GRT. The basis of the estimate is 800 ships and a total of 25,000,000 GRT at the ASP rate of $0.25 per report. If these ships all reported once every 24 hours, that would be 800 x 365 x $0.25 = $73,000 / 25,000,000 = 0.00292 per GRT, roughly $0.003 per GRT. If the Flag State no longer pays for the reports when access is authorized to a Port or Coastal State, this cost could be mitigated to some extent.

**Financial/Accounting Matters**

The settlement of invoices between Contracting Governments, LRIT data providers, and/or the LRIT Data Centre(s) must be defined. The accounting problems can potentially create barriers to putting the LRIT system into operation.

Billing system and principles of accounting can be fairly complicated. The complexity of the accounting system for LRIT Data Centre(s) will likely increase with the number of LRIT Data Centres. The accounting between national LRIT Data Centres may have differences, such as:

- LRIT information costs may be different due to different equipment on ships using different LRIT service providers;

- Within individual countries, LRIT services may have different message pricing as well as the price for maintenance of a national LRIT Data Centre(s). The price per vessel data report could differ from Centre to Centre.

**Conclusions**

LRIT costs are highly dependent on frequency of reports, per message costs (which may be dependent on frequency of reports), quantity of information content, regular vs. on-demand reporting, level of use by Contracting Governments, etc.

There appears to be a limited scope of existing available technologies for LRIT. Based on the premise that such potential available technologies "should not require ships to fit additional or new equipment ...", these available technologies include:

- GMDSS equipment
- SSAS equipment
- Satellite-based communications systems
- Value-added application service providers (e.g., fleet management systems)
- Non-satellite-based communications providers

Based on limited estimates, it appears that per message costs will run in the $.05(USD) - $1.00 (USD). To reiterate the decision of MSC, Contracting Governments will cover all communication costs associated with the provision of LRIT information. The value of LRIT information is only likely to be calculable when comparing the cost to Administrations of monitoring maritime traffic through other means (including physical tracking and interception). This calculus will also need to factor in the cost of delays to maritime fleet operators if they are delayed permission to approach ports. Such data is not freely available, and probably beyond the scope of this analysis.

## TASK 14: LRIT REPORTING PARAMETERS

### 1 Summary of MSC 80's conclusions and guidance to the Correspondence Group

Consider the reporting parameters necessary to allow SOLAS Contracting Governments to obtain LRIT information to which they are entitled.

### 2 Background material

MSC 80/WP.7/Add.1 paragraph 30
MSC 80/WP.7/Add.1 paragraphs 25 and 27;
MSC 8/5/9, Marshall Islands submission;
MSC 8/5/J.20, Marshall Islands presentation; and
Task #10: LRIT Data Centre List of Ships

### 3 Correspondence Group's response

Contracting Governments will have at their disposal several possible methods of interfacing with the LRIT Data Centre, including:

- Web application interface (low-cost, requiring only an internet-enabled computer),
- Local specialized client (medium cost, requiring a dedicated PC-based workstation product), or
- LRIT information routing to a national facility, i.e. National-VMS, local port VMS (high-cost).

Contracting Governments will select from the LRIT Data Centre operator their preferred interface method from the list defined in (1.) above. Each interface method has its own merits, however, as learned through the Marshall Islands LRIT Project, the web application interface architecture worked very well and is the suggested method to develop as the baseline system (from which other, more advanced interfaces can be developed if necessary). Web access affords to Contracting Governments having very little or zero established capability access to LRIT information in equal measure to Contracting Governments that have already established advanced National Vessel Monitoring Systems-type capabilities, thus creating a level playing field.

The LRIT Data Centre will provide Contracting Governments with its e-mail address by which official information would be supplied and requests made to it.

Each Contracting Government will be required to provide the LRIT Data Centre with its Flag, Port and Coastal authority Point(s) of Contact (PoC) information and associated e-mail address(es) for the routing of position reports. The LRIT Data Centre will establish State account(s) for Flag, Port, and/or Coastal State purposes and provide respectively assigned Username(s) and Password(s) to the State Point(s) of Contact by which tracking data would be accessed from the LRIT Data Centre.

*LRIT Data Centre Datafile Specification*

A range of proprietary datafile formats are used to transfer "request" information between third-party users and commercial LRIT ASP systems. The formats are typical and could be adopted for use between States and the LRIT Data Centre. Alternatively, an equivalent XML derivative could be developed based upon the following core elements:

The core elements of the datafile format will be embedded in the e-mail message *header* issued between States and the LRIT Data Centre, and include the:

- **Request Type** (see bullets below),
- **Origin State UNLOCODE**
- **IMO Number** (of the ship concerned).

Each request type would define:

- *the* **Origin State-Type**;
  - Flag
  - Port
  - Coastal, and

- *the* **Request Action**:
  - Integration
  - Transfer
  - Notice, and

- *the* **Action Status**:
  - Request
  - reJection
  - Query
  - Complete
  - Arrival
  - Extension
  - Interest
  - decliNe
  - Deletion
  - Terminated.

The body of a request would concern specifics about the ship and its movement. Each request type would be unique, so e.g., "PTR" would indicate a 'Port Transfer Request'. For audit trail purposes, and to provide an additional validation measure, all requests will be copied to all applicable parties in the communication chain.

*Flag State Data Access Process and Permissions*

During initial fleet registration and integration into the LRIT Data Centre – refer to Task 10 for specifics – the presented ship details will be compared against an on-line service such as Lloyd's Marine Intelligence Unit (LMIU) or Lloyd's Register-Fairplay (LRF). Note: all ships shall be registered to, and integrated with, the LRIT Data Centre irrespective of actual Flag State LRIT operations i.e. even if a Flag State elects not to take advantage of regulatory LRIT the ship must also be technically integrated into the LRIT Data Centre to allow tracking by Port and Coastal States. A positive match will pass the request to the next stage while a negative match will result in a 'Flag Integration reJection' (FIJ) e-mail issued back to the Flag State providing appropriate reason/diagnostics i.e. invalid IMO number. This stage validates the authenticity of the Flag State integration in respect of ship details.

Access to global LRIT information with respect to its own-flagged ships will then be made available from the LRIT Data Centre. In cases where a Flag State has its own N-VMS, the

LRIT information will be routed in real-time from the LRIT Data Centre to the N-VMS. Otherwise LRIT information management systems will be provided by the LRIT Data Centre in the form of a web application interface or standalone local system.

After initial integration into the LRIT Data Centre, Flag State losses and gains will be strictly controlled to ensure that the information supplied is correct and from authorized users. Several checks and balances will be built into the re-integration process to ensure that only legitimate ship additions and deletions are made and the integrity of the LRIT information is maintained.

At stage 2, the ship details will be checked for duplicate entries or pre-existing data under another Flag State (due to buying/selling of ships and addition of newbuildings). A positive match will result in a 'Flag Integration reJection' (FIJ) e-mail issued back to the Flag State providing appropriate reason/diagnostics i.e. duplicate IMO number, while a negative match will result in full integration of the ship into the Flag State account and issuance of a 'Flag Integration Complete' (FIC) e-mail to the Flag State (optional) and Company PoC's. This stage validates the uniqueness of the ship details. The ship then would be available to the Flag State for tracking.

At stage 3, it would be assumed that a change of Flag has occurred, and the 'Flag Integration Deletion' (FID) and 'Flag Integration Request' (FIR) reports have been received by the LRIT Data Centre in close proximity to each other (see Task 10). The change of flag procedures would involve:

- A FID e-mail from a losing Flag State to the LRIT Data Centre server being matched with a FIR from a gaining Flag State, receipt acknowledged by the LRIT Data Centre,

- With a match, the LRIT Data Centre then deleting the ship from the losing Flag State account issuing a FIT e-mail back to the losing Flag State, and

- The LRIT Data Centre adding the ship to the gaining Flag State account issuing a 'Flag Integration Complete' (FIC) e-mail back to the gaining Flag State.

In the event that either one of the reports is received in isolation from the other, the applicable report would be placed in a 'temporary holding area' awaiting receipt of, and for cross referencing with, the associated report. A time threshold would be placed on the duration of this holding period after which an e-mail would be sent to the 'out of synch' request indicating that it is on temporary hold awaiting the matching request. In the event that an associated report is not received, any further action to be taken would have to be determined by the requesting party. This could occur, for example, when a ship is recycled, which may require validation from some other source. Reference should be made to Task 10 for details required from losing and gaining Flag States and the matching protocol required before deletion and re-integration would take place.

The baseline automatic position-reporting interval for a ship would be set (current thinking each 24 hours); however, during the tracking period, the Flag State would be allowed at any time to poll a ship for an on-demand position report and to modify the automatic position-reporting interval (between 5 minutes and 24 hours). There would be no tracking end-date/time. This would only occur on the occasion of a validated notice of deletion from the flag received from the Flag State for whatever reason.

To establish an account with the LRIT Data Centre and subsequently access that account, Flag States would use the LRIT Data Centre e-mail address and datafile format to:

- Provide the State UNLOCODE;
- Identify a Flag State authorized Point of Contact;
- Specify a PoC e-mail address for ship integration communications and validation;
- Provide initial fleet installation data (see Task 10);
- Specify a baseline automatic position reporting interval;
- Specify any Port State or Coastal State exclusions; and then
- Utilize the username and password assigned to the State PoC to access its LRIT Data Centre tracking service account.

*Port State Data Access Process and Permissions*

Port State access to Flag State ships shall be strictly controlled in much the same way as Flag State access to its own ships in order that the LRIT information is made available to legitimate authorized users only. It is anticipated that Port State access to LRIT information will be integrated – both technically and in a legal context - within the various national Advanced Notice of Arrival (ANOA) frameworks.

In the first instance, the Port State will issue a 'Port Transfer Request' (PTR) e-mail identifying itself by UNLOCODE and the specific ship details by IMO number, Name, destination port UNLOCODE and ETA (as provided in the ANOA). The Port State e-mail address and its associated UNLOCODE will be compared to that pre-registered by the Port State and held by the LRIT Data Centre. A positive match will pass the request to the next stage while a negative match will result in a 'Port Integration reJection' (PIJ) e-mail issued back to the Port State providing appropriate reason/diagnostics i.e. invalid UNLOCODE. This stage validates the authenticity of the Port State.

At stage 2, the ship IMO number and Name will be compared to that pre-registered by the Flag State and held by the LRIT Data Centre. A positive match will pass the request to the next stage, while a negative match process will result in a PIJ e-mail. This stage validates the authenticity of the Ship.

At stage 3, Flag-Port State exclusions will be checked against pre-registered instructions (*none are anticipated at this stage). A positive match will result in a PIJ e-mail. A negative match will result in integration of the ship into the requesting Port State account, and the simultaneous issuance of a 'Port Transfer Complete' (PTC) e-mail to the Port State, Flag State (optional), and Company PoC's (in the case of the Company PoC/CSO for passive validation). This stage validates the regulatory authenticity of the request.

Under nominal conditions no action will be required of the Company PoC/CSO; however, in the event that an inconsistency is observed in the PTC, the CSO may issue a Port Transfer Query (PTQ) e-mail, whereupon the ship will be placed in a 'temporary holding area' pending resolution of the query. Note: national variations in ANOA form structures and reporting methods (e-mail attachment, fax, on-line) preclude 'cc-ing' of the original ANOA submission to the LRIT Data Centre for this validation purpose.

The baseline automatic position-reporting interval will be re-set to that of the Port State (current thinking is each 4 hours). However, during the tracking period, the Port State will be allowed at any time to poll the ship for an on-demand position report and to modify the automatic position-reporting interval (between 5 minutes and 24 hours). Bearing in mind that the intent of LRIT should be to track ships to within the range of AIS or VTS networks, the tracking end-date/time would be set to the ship's ETA, at which time the LRIT Data Centre would delete the ship from the Port-State account and issue a 'Port Transfer Terminated' (PTT) e-mail to the Port State, Flag State (optional), and Company PoC's. However, if the Port State considered that the original ETA was sufficiently inaccurate as to result in a premature PTT, a 'Port Transfer Extension' (PTE) may be requested by e-mail to set the tracking duration to a revised ETA.

To establish an account with the LRIT Data Centre and subsequently access that account, Port States would use the LRIT Data Centre e-mail address and datafile format to:

- Provide its UNLOCODE;
- Identify a Port State authorized Point of Contact;
- Specify a PoC e-mail address for ship integration communications and validation;
- Specify a default automatic position reporting interval, and then
- Utilize the username and password assigned to the PoC to access its LRIT Data Centre tracking service account.

*Coastal State Data Access Process and Permissions*

Coastal State access (to Flag State ships) would be strictly controlled using 'Coastal State Zones' (CSZs) at the LRIT Data Centre level to ensure that LRIT information is made available to legitimate authorized users only. It is anticipated that Coastal State access will be based on National requirements established within the confines of the proposed SOLAS amendment and may vary across Contracting Governments (current thinking 200-2000 nm).

The CSZ may or may not correspond to the same Contracting Government's Port State ANOA tracking zone. The speed of advance and the course track of a ship will definitely be factors to consider. Since both may vary significantly with the innocent passage or approach of a ship, routine periodic satellite wide-area synoptic "pinging" may be the correct approach to take, especially in detecting the presence of and identifying ships on innocent passage with no intentions of making a port call within a CSZ. This method, in conjunction with an appropriate level of historical tracking (current thinking each 24 hours), would preclude the need for ships to transmit course and speed.

At all times, the LRIT Data Centre will compare each responding position report against a look-up table of CSZs and perform an 'inside/outside' calculation. An initial 'inside' match when having entered a CSZ will result in the ship details being compared against the regulatory permissions table to establish if there were any Coastal State exclusions being imposed by its Flag State (a persistent 'outside' match would result in no further action, i.e. neither inside nor departing a zone). A negative match during the exclusion check will result in temporary integration of the ship into a Coast State account and the issuance of a 'Coastal Transfer Interest' (CTI) e-mail being sent to the Coastal State PoC.

The Coastal State PoC, upon receiving the notice and request for interest from the LRIT Data Centre, will acknowledge same by either declaring 'Coastal Transfer decliNe' (CTN) whereupon no further action would take place, or by making a 'Coastal Transfer Request' (CTR), which will result the in temporary integration of the ship into the Coast State account making the ship available to the Coastal State for tracking. The automatic position-reporting interval will be re-set (current thinking each 4 hours), and issuance of a 'Coastal Transfer Complete' (CTC) e-mail to the Coastal State, Flag State (optional), and Company (optional) PoC's.

During the tracking period (a persistent 'inside' match), the Coastal State could at any time poll the ship for an on-demand position report and to modify the automatic position-reporting interval (between 5 minutes and 24 hours), or terminate the coastal tracking altogether by requesting a 'Coastal Transfer Deletion' (CTD). An initial 'outside' match when having departed a CSZ will result in the LRIT Data Centre deleting the ship from the Coastal State account and issuance of a 'Coastal Transfer Terminated' (CTT) e-mail to the Coastal State, Flag State (optional), and Company (optional) PoC's..

To establish an account with the LRIT Data Centre and subsequently access that account, Coastal States will use the LRIT Data Centre e-mail address and datafile format to:

- Identify a Coastal State authorized Point of Contact;
- Specify a PoC e-mail address for ship integration communications and validation;
- Provide detailed polygonal co-ordinates of the Coastal State Zone;
- Specify a default automatic position reporting interval, and then
- Utilize the username and password assigned to the PoC to access its LRIT Data Centre tracking service account.

*Conceptual Layered Strategy*

The Flag-Port-Coastal State concept of operations is described above in three discrete stages. It should be noted, however, that in reality a Port Transfer Termination (PTT) based on ETA, or extended ETA, is only an interim termination. When the ship departs a port, it would either be:

- Destined for another port under the jurisdiction of the same Port State in which case the ship should have submitted another ANOA and so would continue in the Port State transit phase, or be
- En-route to a port outside the jurisdiction of the Port State in which case the ship transfers into a Coastal State transit phase until the CSZ is exited.

There is one more technical issue to be sorted out at the LRIT Data Centre level. Because there will be multiple automatic position-reporting intervals registered with the system, e.g. Flag State at one rate, then Port States and Coastal States at others, the system should allow the higher rate to pre-empt the lower rate and be chargeable to the party requiring the higher rate while still allowing the lower rate user to passively track a ship, unless specifically poled for a position report.

_____